Wireless Networks Physical Layer Security: Modeling and Performance Characterization

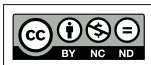
by

Long KONG

MANUSCRIPT-BASED THESIS PRESENTED TO ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
IN PARTIAL FULFILLMENT FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
Ph.D.

MONTREAL, MAY 29, 2019

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC



BOARD OF EXAMINERS

THIS THESIS HAS BEEN EVALUATED

BY THE FOLLOWING BOARD OF EXAMINERS

M. Georges Kaddoum, Thesis Supervisor
Department of Electrical Engineering, École de technologie supérieure

M. Chamseddine Talhi, President of the Board of Examiners
Department of Software Engineering and Information Technologies, École de technologie supérieure

M. François Gagnon, Member of the jury
Department of Electrical Engineering, École de technologie supérieure

M. Maged ElKashlan, External Independent Examiner
School of Electronic Engineering and Computer Science, Queen Mary University of London

THIS THESIS WAS PRESENTED AND DEFENDED

IN THE PRESENCE OF A BOARD OF EXAMINERS AND THE PUBLIC

ON "14, MAY, 2019"

AT ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

FOREWORD

This dissertation is mainly based on the research outcomes, which are accomplished under the supervision of Dr. Georges Kaddoum from February 2015 to May 2019. This work is financially supported by the research chair of physical layer security in wireless networks. This dissertation is subjective to address the secure concern of physical layer security over several general but useful fading channel models. Resultantly, my Ph.D. study successfully ended with 7 journal papers published, 4 IEEE international conference papers published and 1 conference paper under review as the first author.

Apart from the first two chapters, where the background of physical layer security are intensely introduced, the remaining chapters are based on my journal papers. For those chapters, I did a comprehensive literature review, reasonably formulated problems, feasibly proposed possible solutions, mathematically analyzed and simulated the performance, and technically draft manuscripts. After the presentation of those chapters, chapter 9 concludes the whole work and lists several future research directions.

ACKNOWLEDGEMENTS

First and foremost, I would like to show my sincere gratitude to my supervisor Dr. Georges Kaddoum for his considerate guidance, valuable inspiration, consistent encouragement, and constructive suggestion throughout my four-year research study. This thesis would not come to the completion without his dedicated mentor and scholarly inputs.

Besides my supervisor, I am also appreciative to Dr. François Gagnon, Dr. Chamseddine Talhi, and Dr. Maged Elkashlan for their agreements to serve as my jury members. Similar, profound gratitude also goes to Dr. Wang for his endless support even after my master's graduation. I am also appreciative to Dr. Nandana Rajatheva's help and support when applying the Mitacs research project. Also, a special mention and thank go to the PERSWADE and Mitacs programs for their finical support of my Ph.D. study and my visit to the Centre for Wireless Communications (CWC), University of Oulu, Finland.

In particularly, I am deeply grateful to Dr. Tran, Dr. Cai, Dr. He, Dr. Daniel, Dr. Zouheir, and Dr. Vuppala for their help and discussions.

Many thanks are also due to my friends for their help to keep me away from depression and encourage me with high enthusiasm to embrace my research problems. I do hereby acknowledge all my colleagues from LaCIME group, including Dawa, Ebrahim, Hamza, Hung, Ibrahim, Jung, Khaled, Nancy, Michael, Sahabul, Tran, Victor, Vu, and Zeeshan etc., my ETS friends, including Ammon, Cha, Huan, Longfei, Jizong, XiaoFan, Xiaohang, MingLi, and Zijian, as well as my friends, including Clark, Cong, Dong, Fei, Hao, Jin, Ting, and Yijing.

Finally, I would like to wholeheartedly thank my parents for their continued patience, unconditional long-term support, and warm love. In particularly, I owe my mother my deepest apology since I was not with her at the last minute of her life, and also she can not share this biggest joy and witness my achievement come true. Also, my special thanks and appreciation to my sisters and brother for their spiritually invaluable support and love to my studies and life.

Sécurité de la couche physique des réseaux sans fil: modélisation et caractérisation des performances

Long KONG

RÉSUMÉ

Poussée par la croissance et l'expansion exponentielles des périphériques sans fil, la sécurité des données joue, de nos jours, un rôle de plus en plus important dans tous nos transactions et interactions quotidiennes avec différentes entités. Des exemples possibles, y compris les informations de santé et les achats en ligne, deviennent très vulnérables en raison de la nature intrinsèque du support de transmission sans fil et de l'ouverture d'accès aux liens sans fil. Traditionnellement, la sécurité des communications est principalement considérée comme étant les tâches traitées au niveau des couches supérieures de la pile de protocoles en couches, les techniques de sécurité, y compris le contrôle d'accès personnel, la protection par mot de passe et le chiffrement de bout en bout. Ces techniques ont été largement étudiés dans la littérature. Plus récemment, le potentiel que présente la couche physique pour améliorer la sécurité des communications sans fil apporte de plus en plus d'intérêt. Etant un paradigme nouveau et attrayant au niveau de la couche physique, la sécurité de la couche physique repose sur deux travaux fondamentaux: (i) la théorie de l'information de Shannon. (ii) le canal d'écoute électronique de Wyner.

Compte tenu des fondements de la sécurité de la couche physique et de la nature différente des divers réseaux sans fil, cette thèse est censée combler davantage le manque qu'on trouve dans les résultats des travaux de recherche existants. En guise de précision, les contributions de cette thèse peuvent être résumées comme suit: (i) exploration des métriques de confidentialité sur des canaux à évanouissement plus généraux; (ii) la caractérisation d'un nouveau modèle de canal à évanouissements et l'analyse de sa fiabilité et de sa sécurité lors de son application aux systèmes de communication numériques; (iii) étude de la sécurité de la couche physique sur les canaux aléatoires MIMO à évanouissement $\alpha - \mu$.

En prenant en compte le modèle d'écoute électronique classique d'Alice-Bob-Eve, la première contribution peut être divisée en quatre parties: (i) nous avons étudié les performances de confidentialité sur des canaux SISO à évanouissement $\alpha - \mu$. La probabilité de capacité de confidentialité non nulle (PNZ) et la limite inférieure de probabilité d'interruption de secret (SOP) sont calculées pour le cas particulier où le canal principal et le canal d'écoute subissent le même paramètre de non-linéarité d'évanouissement, à savoir, α. Par la suite, afin de combler le manque d'expression de forme fermée de la SOP dans la littérature et d'étendre les résultats obtenus au chapitre 2 pour le cas des canaux d'écoute SIMO à évanouissement $\alpha - \mu$. En utilisant le fait que les rapports signal sur bruit (SNR) reçus au niveau du récepteur légitime et au niveau de l'écoute clandestine peuvent être approchés en tant que nouvelles variables aléatoires (RV) de distribution $\alpha - \mu$, la métrique SOP est donc dérivée et donnée en termes de la fonction H bivariée de Fox ; (ii) la performance de confidentialité sur les canaux d'écoute électronique Fisher-Snedecor F à évanouissement est initialement prise en compte. Les SOP,

PNZ et ASC sont finalisées en termes de fonction G de Meijer (iii) afin de généraliser les résultats obtenus sur F canaux d'écoute électronique de Fisher-Snedecor à évanouissement $\alpha-\mu$, un canal à évanouissement plus flexible et plus général, comme le modèle d'atténuation de la fonction H de Fox, est pris en compte. Les analyses exactes et asymptotiques de SOP, PNZ et al capacité de confidentialité moyenne (ASC) sont développées avec des expressions de forme fermée; (iv) Enfin, motivés par le fait que la distribution MG (mélange gamma) est un outil attrayant, qui peut être utilisé pour modéliser les SNRs reçus instantanément sur des canaux sans fil à évanouissements, les métriques de confidentialité sur divers canaux d'écoute électronique à évanouissements sont dérivées en utilisant l'approche MG.

En raison de la puissance de transmission et de la portée de communication limitées, les relais coopératifs ou les réseaux sans fil à sauts multiples sont généralement considérés comme deux moyens prometteurs pour résoudre ces problèmes. Inspiré par les résultats obtenus aux chapitres 2 et 3, le second apport consiste à proposer un modèle de canal à évanouissements novateur mais simple, à savoir le cascadé $\alpha-\mu$. Cette nouvelle distribution est avantageuse puisqu'elle englobe facilement les canaux cascadés existantes Rayleigh, Nakagami-m et Weibull. Sur cette base, les performances de fiabilité et de confidentialité d'un système numérique sur des canaux de fading $\alpha-\mu$ en cascade sont ensuite évaluées. Les expressions en forme fermée des mesures de fiabilité (y compris la quantité d'atténuation (AF), la probabilité de coupure, la capacité moyenne du canal et la probabilité d'erreur de symbole moyenne (ABEP)) ainsi que les mesures de confidentialité (y compris SOP, PNZ et ASC) sont fournies. En outre, leurs comportements asymptotiques sont également effectués et comparés aux résultats exacts.

Considérant les effets de la densité des utilisateurs, de la distribution spatiale et du facteur d'affaiblissement de propagation sur la confidentialité de la communication, le troisième aspect de cette thèse est détaillé dans le chapitre 8 en tant qu'investigation sur la confidentialité du système MIMO stochastique sur des canaux d'écoutes électroniques avec évanouissement $\alpha-\mu$. La géométrie stochastique et le schéma de transmission spatio-temporelle classique (STT) sont utilisés dans la configuration du système. La question de la confidentialité est évaluée mathématiquement par le biais de trois métriques, à savoir la coupure de connexion, la probabilité de la capacité de confidentialité non nulle et la capacité de confidentialité ergodique. Ces trois métriques sont ensuite dérivées en termes de deux schémas de classement et comparées ensuite aux simulations de Monte-Carlo.

Mots-clés: sécurité de la couche physique, $\alpha-\mu$, Fisher-Snecedor $\mathscr{F}$, fonction H de Fox, distribution gamma mixte (MG), $\alpha-\mu$ cascadé, réseau MIMO stochastique

Wireless Networks Physical Layer Security: Modeling and Performance Characterization

Long KONG

ABSTRACT

Intrigued by the rapid growth and expand of wireless devices, data security is increasingly playing a significant role in our daily transactions and interactions with different entities. Possible examples, including e-healthcare information and online shopping, are becoming vulnerable due to the intrinsic nature of wireless transmission medium and the widespread open access of wireless links. Traditionally, the communication security is mainly regarded as the tasks at the upper layers of layered protocol stack, security techniques, including personal access control, password protection, and end-to-end encryption, have been widely studied in the open literature. More recently, plenty of research interests have been drawn to the physical layer forms of secrecy. As a new but appealing paradigm at physical layer, physical layer security is based on two pioneering works: (i) Shannon's information-theoretic formulation and (ii) Wyner's wiretap formulation.

On account of the fundamental of physical layer security and the different nature of various wireless network, this dissertation is supposed to further fill the lacking of the existing research outcomes. To be specific, the contributions of this dissertation can be summarized as three-fold: (i) exploration of secrecy metrics to more general fading channels; (ii) characterization a new fading channel model and its reliability and security analysis in digital communication systems; and (iii) investigation of physical layer security over the random multiple-input multiple-output (MIMO) $\alpha-\mu$ fading channels.

Taking into account the classic Alice-Bob-Eve wiretap model, the first contribution can be divided into four aspects: (i) we have investigated the secrecy performance over single-input single-output (SISO) $\alpha-\mu$ fading channels. The probability of non-zero (PNZ) secrecy capacity and the lower bound of secrecy outage probability (SOP) are derived for the special case when the main channel and wiretap channel undergo the same non-linearity fading parameter, i.e., α. Later on, for the purpose of filling the gap of lacking closed-form expression of SOP in the open literature and extending the obtained results in chapter 2 to the single-input multiple-output (SIMO) $\alpha-\mu$ wiretap fading channels, utilizing the fact that the received signal-to-noise ratios (SNRs) at the legitimate receiver and eavesdropper can be approximated as new $\alpha-\mu$ distributed random variables (RVs), the SOP metric is therefore derived, and given in terms of the bivariate Fox's H-function; (ii) the secrecy performance over the Fisher-Snedecor $\mathscr{F}$ wiretap fading channels is initially considered. The SOP, PNZ, and ASC are finalized in terms of Meijer's G-function; (iii) in order to generalize the obtained results over $\alpha-\mu$ and Fisher-Snedecor $\mathscr{F}$ wiretap fading channels, a more flexible and general fading channel, i.e., Fox's H-function fading model, are taken into consideration. Both the exact and asymptotic analysis of SOP, PNZ, and average secrecy capacity (ASC), are developed with closed-form expressions; and (iv) finally, motivated by the fact that the mixture gamma (MG) distribution is

an appealing tool, which can be used to model the received instantaneous SNRs over wireless fading channels, the secrecy metrics over wiretap fading channels are derived based on the MG approach.

Due to the limited transmission power and communication range, cooperative relays or multi-hop wireless networks are usually regarded as two promising means to address these concerns. Inspired by the obtained results in Chapters 2 and 3, the second main contribution is to propose a novel but simple fading channel model, namely, the cascaded $\alpha-\mu$. This new distribution is advantageous since it encompasses the existing cascaded Rayleigh, cascaded Nakagami-*m*, and cascaded Weibull with ease. Based on this, both the reliability and secrecy performance of a digital system over cascaded $\alpha-\mu$ fading channels are further evaluated. Closed-form expressions of reliability metrics (including amount of fading (AF), outage probability, average channel capacity, and average symbol error probability (ABEP).) and secrecy metrics (including SOP, PNZ, and ASC) are respectively provided. Besides, their asymptotic behaviors are also performed and compared with the exact results.

Considering the impacts of users' densities, spatial distribution, and the path-loss exponent on secrecy issue, the third aspect of this thesis is detailed in Chapter 8 as the secrecy investigation of stochastic MIMO system over $\alpha-\mu$ wiretap fading channels. Both the stochastic geometry and conventional space-time transmission (STT) scheme are used in the system configuration. The secrecy issue is mathematically evaluated by three metrics, i.e., connection outage, the probability of non-zero secrecy capacity and the ergodic secrecy capacity. Those three metrics are later on derived regarding two ordering scheme, and further compared with Monte-Carlo simulations.

Keywords: Physical layer security, $\alpha-\mu$, Fisher-Snecedor $\mathscr{F}$, Fox's H-function, mixture gamma (MG) distribution, cascaded $\alpha-\mu$, stochastic MIMO network

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABREVIATIONS

AF	amplify-and-forward
AN	artificial noise
AoF	amount of fading
ASC	average secrecy capacity
ASEP	average symbol error probability
AWGN	additive white Gaussian noise
BFSK	binary frequency-shift keying
BPSK	binary phase shift keying
CCDF	complementary cumulative distribution function
CDF	cumulative distribution function
COP	connection outage probability
CSI	channel state information
DBPSK	differential binary phase shift keying
D2D	device-to-device
EGK	extended generalized-$\mathscr{K}$
FSO	free space optical
HPPP	homogeneous Poisson point process
ICT	information and communication technology
i.i.d.	independent and identically distributed

mmWave	millimetrewave
M-QAM	quadrature amplitude modulation
M2M	mobile-to-mobile
MG	mixture gamma
MGF	moment-generating function
MIMO	multiple-input multiple-output
MISO	multiple-input single-output
NOMA	nonorthogonal multiple access
PDF	probability density function
PPP	Poisson point process
PLS	Physical layer security
PNZ	probability of non-zero secrecy capacity
QAM	quadrature amplitude modulation
QPSK	quadrature phase shift keying
RFID	radio-frequency identification
RV	random variable
SER	symbol error rate
SIMO	single-input multiple-output
SISO	single-input single-output
SNR	signal-to-noise ratio

SOP	secrecy outage probability
SR	security region
STT	space-time transmission
V2V	vehicle-to-vehicle
WBAN	wireless body area networks
ZF	zero-forcing
5G	fifth-generation

LISTE OF SYMBOLS AND UNITS OF MEASUREMENTS

$(\cdot)^+$	max(0,x)
dB	Decibel
x	Variable
$\mathbf{x}$	Vector
$\mathbf{X}$	Matrix
lim	Limits
$\mathscr{E}$	Expectation operator
$\mathscr{V}$	Variance operator
$\mathscr{B}(\cdot,\cdot)$	Beta function
$\exp(\cdot)$	Exponential function
$\log_2$	Logarithm with base 2
ln	Natural logarithm
$\Gamma(\cdot)$	Gamma function
$\gamma(\cdot,\cdot)$	Upper incomplete gamma function
$\Gamma(\cdot,\cdot)$	Lower incomplete gamma function
${}_2F_1(\cdot,\cdot;\cdot;\cdot)$	Gaussian hypergeometric function
$\Psi(\cdot)$	Diagamma function
$\mathrm{Res}(f(x),s)$	The residue of function $f(x)$ at pole $x=p$
$H_{p,q}^{m,n}(\cdot)$	Univariate Fox's H-function

$G_{p,q}^{m,n}(\cdot)$	Univariate Meijer's G-function
$H_{p,q;p_1,q_1;p_2,q_2}^{m,n;m_1,n_1;m_2,n_2}(\cdot)$	Bivariate Fox's H-function
$G_{p,q;p_1,q_1;p_2,q_2}^{m,n;m_1,n_1;m_2,n_2}(\cdot)$	Bivariate Meijer's G-function

INTRODUCTION

As stated in the report of Ericsson entitled "10 hot consumer trends 2019" Ericsson (2018), technology does make our daily life cheaper, easier, and more convenient. Specifically, supermarkets without checkouts; schools with increasing robotization of teachers and hospitals with non-human doctors; restaurants with mechanized menus; and cars with non-human drivers are just few already being realized possibilities. These examples are obvious the applications of ICT. The services provided are implemented by using the wireless transmission medium. However, the openly accessible physical nature of radio links makes the legitimate links vulnerable. Thus, the ever-increasing services provided by ICT come with an unavoidable security concern. It is also highlighted in the aforementioned report that 52% of consumers think most popular apps collect more smartphone data than needed in order to make profits. Resultantly, safeguarding our confidential messages from being intercepted or misused is a challenging problem Jameel, F., Wyne, S., Kaddoum, G. & Duong, T. Q. (2018); Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. & Ghani, N. (2019).

Communication security concerns exist as long as there are wireless communication links. Dating back to the ancient times, either flags or flames were used to deliver battlefield information. As a consequence, enemies were easily able to access the information. The security concern of how to provide high data confidentiality from head to toe arose. In the recent war era, encrypted telegraph was widely used to convey important messages. In this context, the only way to decrypt the cipher text is to know the encryption scheme. Therefore, the decryption process is time-consuming even if the cipher texts are at hand. The encryption philosophy is also employed to enhance the security of wireless networks.

Taking a glance at the layered protocol stack, technical solutions, such as personal access controls (fingerprints, face recognition, watermark), password protection, authorization, and end-to-end encryption, are widely employed for keeping eavesdroppers and attackers away.

Although seemingly effective, these techniques still present many limitations. For example, the most popular encryption methods, such as AES and RSA, are key-based solutions, this kind of solutions are based on the assumptions that the one way functions are difficult to break, in other words, this means that unauthorized devices have insufficient computational capabilities for decryption; obviously, this assumption is increasingly losing its validity due to the exponential growth of the users' computational ability. Also, devices are connected to the network with different power, and they join in or leave the network randomly, due to the decentralized nature of future wireless networks Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J. & Di Renzo, M. (2015). As a consequence, key management and distribution are becoming challenging. For those reasons, the downsides of key-based solutions become apparent:

- low spectrum efficiency due to the transmission of additional headers and data;
- high computation and battery consumption, especially for public key based solutions;

In addition, the rapid growth of computational devices makes it adequately possible for eavesdroppers to have sufficient computational capabilities against the mathematical assumption (e.g., factorizing large integers). Besides, the current and future wireless network topologies are becoming decentralized. Moreover, random distributed users with different power and computational abilities can access the wireless network. Resultantly, key generation and management become increasingly challenging.

To this end, the attempts of merely relying on the upper layers security enhancement solutions are no longer a wise and perfect policy. In addition, recent research attention shifted from the upper layers to the physical layer due to Shannon's original information-theoretic establishment and Wyner's degraded wiretap channel formulation. As a new framework, physical layer security is appealing and promising, since it is not based on cryptography algorithms or secret keys (though they might support such solutions.). The essence of physical layer security is to

smartly exploit the intrinsic randomness of wireless medium to reversely secure the legitimate transmission links Bloch, M. & Barros, J. (2011); Zhou, X., Song, L. & Zhang, Y. (2016).

Problem Statement and Motivations

Over the years, the emergence of various wireless networks, such as cognitive radio networks, wireless sensor networks, mobile-to-mobile (M2M) networks, device-to-device (D2D) communications, wireless body area networks (WBAN) Chong, P. K., Yoo, S. E., Kim, S. H. & Kim, D. (2011); Moosavi, H. & Bui, F. M. (2016), and many others, has attracted plenty of research interests from the wireless communication and signal processing communities. Due to the uniqueness characteristics of each communication scenario, many novel fading channel models appear to meet their requirements.

For examplem, as stated in the literature, the $\alpha - \mu$ fading channel was proposed in 2008 to model the small-scale fading of wireless links. Later on, it was proved to be valid for the WBAN, and Vehicle-to-Vehicle (V2V) communication scenarios Jeong, Y., Chong, J. W., Shin, H. & Win, M. Z. (2013); Wu, Q., Matolak, D. W. & Sen, I. (2010). Similarly, the Fisher-Snedecor $\mathscr{F}$ fading channel was proposed to model the composite fading, and it was verified to accurately characterize the D2D communication links at 5.8 GHz in both indoor and outdoor environments. Since both $\alpha - \mu$ and Fisher-Snedecor $\mathscr{F}$ have their own characteristics when applying to different communication scenarios. For this reason, a fairly general and flexible fading model is needed to compensate the most or all the existing fading models. To address this issue, one possible promising candidate is the Fox's H-function distribution. In this thesis, we have demonstrated that the Fox's H-function distribution can be easily tailored to emulate the $\alpha - \mu$, the Fisher-Snedecor $\mathscr{F}$, cascaded $\alpha - \mu$ fading models, and many other fading distributions as special cases.

Following the aforementioned discussion, in this thesis, we explored the secrecy concern over this generalized wireless fading channels from the information-theoretic perspective.

Research Objectives

In this thesis, we will focus on the investigation of physical layer security over the $\alpha - \mu$, Fisher-Snedecor $\mathscr{F}$, and Fox's H-function fading channels. Three key secrecy metrics, including the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), and the average secrecy capacity (ASC), are developed for the purpose of (i) providing mathematical computational tools for wireless communication engineers to quickly access and subsequently evaluate the security risk; and (ii) enabling network designers to degrade the quality of received signals at the malicious users or devices.

Bearing this objective in mind, we have introduced the Parseval's relation for Mellin transform to formulate the aforementioned secrecy metrics with consideration of the classic Alice-Bob-Eve wiretap channel. This useful relation is fairly beneficial since it enables us to have closed-form tractable expressions for all the secrecy metrics.

Besides, the MG distribution is also introduced as a powerful tool to model the received SNRs over wireless channels, and subsequently applied herein to characterize the secrecy performance.

In order to consider more complex scenarios, studies are also conducted to characterize the physical layer security over the cascaded $\alpha - \mu$ wiretap channel. In addition, physical layer security of random wireless MIMO $\alpha - \mu$ fading channels are subsequently explored, where the impacts of path-loss exponent, fading conditions, and ordering policies, are well discussed.

Contributions and Outline

The dissertation is structured as shown in Fig. 0.1, and detailed as follows.

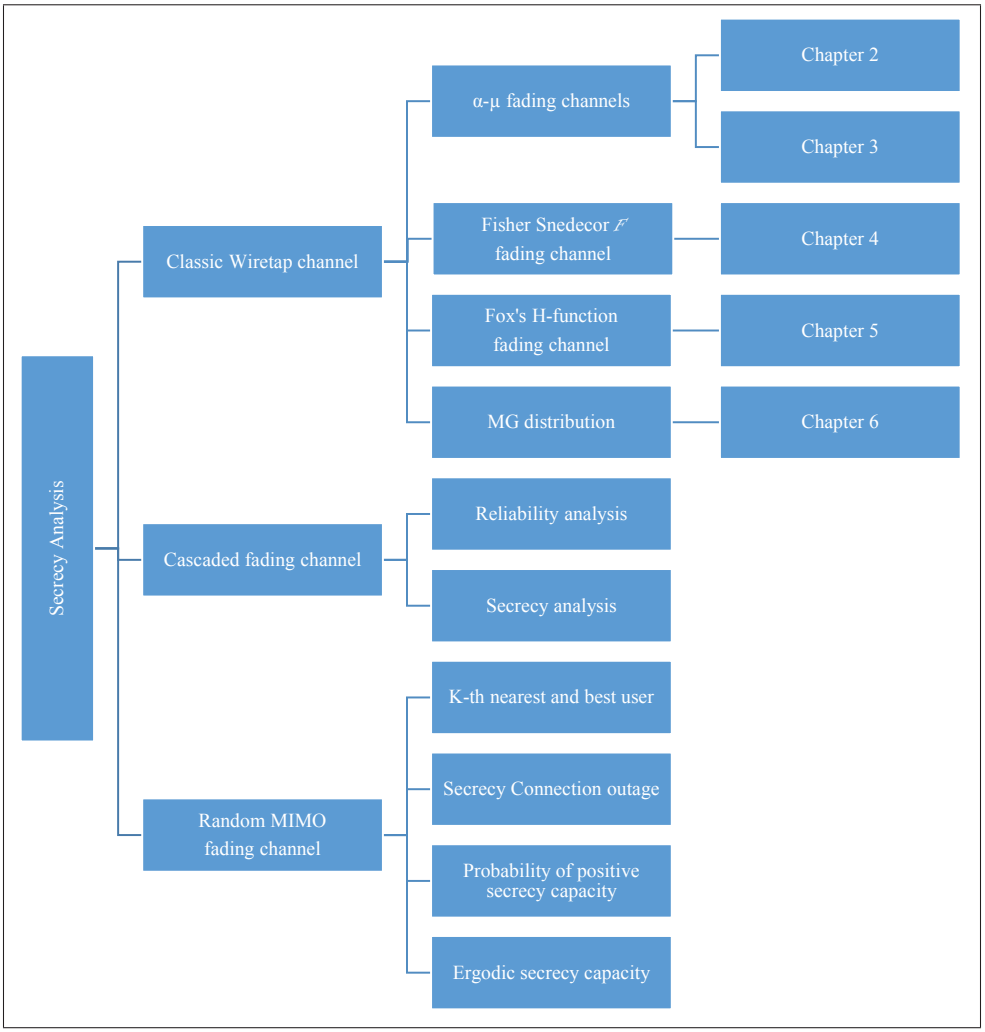


Figure 0.1 The paradigm of thesis contribution

Chapter 1 briefly introduces the state-of-arts of physical layer security and the tools used in this thesis. Chapters 2 and 3 investigate the SOP over single-input single-output (SISO) and single-input multiple-output (SIMO) $\alpha - \mu$ wiretap fading channels, respectively. Precisely, the SOP and the PNZ are derived with closed-form expressions.

Chapter 4 investigates the physical layer security over Fisher-Snedecor $\mathscr{F}$ fading channels, where the SOP, PNZ and ASC, are derived in closed-form. The asymptotic behavior of the

ASC are also analyzed to provide a relatively simpler form for specific cases. Simulation results are presented to validate the accuracy of our analytical results.

In continuation with the previous three chapters, we have further considered a more general and flexible fading channel model in Chapter 5, namely, the Fox's H-function fading model. The main contribution of this chapter is three-fold. First, we have derived the closed-form expressions for the three key secrecy metrics; Second, the asymptotic behaviors of those three metrics are also provided in a simple and accurate mathematical form, especially for several extreme cases; Third, we also investigate the secrecy performance in the presence of colluding eavesdroppers. The so-called super eavesdropper is taken into consideration, and the MRC and SC schemes are applied and further compared when evaluating secrecy performance for the colluding eavesdropping scenario. For the sake of verifying the obtained novel results, three general fading models, including the $\alpha-\mu$, the Fisher-Snedecor $\mathscr{F}$, and the extended generalized-$\mathscr{K}$ distributions, are taken into consideration.

In addition to the aforementioned contributions, the Mixture Gamma (MG) distribution, which is used to flexibly model the legitimate and illegitimate received signal-to-noise ratios (SNRs) over various wireless channels, is considered in Chapter 6, where the secrecy metrics are developed with closed-form expressions, and further validated by Monte Carlo simulations over three fading channels.

In Chapter 7, we propose a novel fading channel model, i.e., the cascaded $\alpha-\mu$ fading channel, which is a promising candidate to the MIMO pinhole or multiple-hop amplify-and-forward (AF) systems' channel modeling. Moreover, both the reliability and secrecy analysis are conducted over the cascaded $\alpha-\mu$ fading channels.

Considering the spatial distribution of users, Chapter 8 deploys the stochastic geometry tool, and analyzes the connection outage probability, the probability of non-zero secrecy capacity,

and the ergodic secrecy capacity of multiple-input multiple-output (MIMO) Wireless Networks over $\alpha - \mu$ Fading Channels. Closed-form mathematical expressions are obtained in terms of Fox's H-function. Useful insights to demonstrating the interactions between different parameters are also provided.

Finally, Chapter 9 concludes this dissertation and presents several possible future research directions.

Author's publication

The outcomes of the author's Ph.D. research are either published or submitted to IEEE journal and conferences, which are listed below with the acronyms "J" for journals and "C" for conferences.

- J1: **Kong L.**, Kaddoum G., and Chergui H., "On Physical Layer Security over Fox's H-Function Wiretap Fading Channels", accepted by *IEEE Trans. Veh. Technol.*, May 2019.

- J2: **Kong L.** and Kaddoum G., "Secrecy Characteristics with Assistance of Mixture Gamma Distribution", accepted by *IEEE Wireless Commun. Lett.*, Mar. 2019.

- J3: **Kong L.**, Kaddoum G., and Rezki Z., "Highly Accurate and Asymptotic Analysis on the SOP over SIMO $\alpha - \mu$ Fading Channels", *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2088-2091, Oct. 2018.

- J4: **Kong L.** and Kaddoum G., "On Physical Layer Security over Fisher-Snedecor $\mathscr{F}$ wiretap fading channels", *IEEE ACCESS*, vol. 6, pp. 39466-39472, Dec. 2018.

- J5: **Kong L.**, Kaddoum G., and Benevides da Costa D., "Cascaded $\alpha - \mu$ Fading Channels: Reliability and Security Analysis", *IEEE ACCESS*, vol. 6, pp. 41978-41992, Dec. 2018.

- J6: **Kong L.** Vuppala S., and Kaddoum G., "Secrecy Analysis of Random MIMO Wireless Networks over $\alpha - \mu$ Fading Channels", *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11654-11666, Sep. 2018.

- J7: **Kong L.**, Tran H., and Kaddoum G., "Performance Analysis of Physical Layer Security over $\alpha - \mu$ Fading Channel", *IET Elec. Lett.*, Vol. 52, no. 1, pp. 45-47, Jan. 2016.

Apart from the afore-listed journal papers that contribute to the main body of this dissertation, the other scientific publications that the author either has been involved in or drafted as the first author are not included in this dissertation, are listed as follows.

- J8: Kaddoum G., Tran H., **Kong L.** and Atallah M., "Design of Simultaneous Wireless Information and Power Transfer Scheme for Short Reference DCSK Communication Systems", *IEEE Trans. Comm.*, Vol. 65, no.1, pp. 431 - 443, Jan. 2017.

- J9: Ai Y., **Kong L.**, and Cheffena M., "Secrecy outage analysis of double shadowed Rician channels", *IET Electron. Lett.*, early access, Apr., 2019.

- C1: **Kong L.**, Ai. Y., He J., Rajatheva. N., and Kaddoum G., "Intercept Probability Analysis over the Cascaded Fisher-Snedecor $\mathscr{F}$ Fading Wiretap Channels", submitted to *IEEE ISWCS*, Aug. 27-30, 2019, Oulu, Finland.

- C2: **Kong L.**, Kaddoum G., and Vuppala S., "On Secrecy Analysis for D2D Networks over $\alpha - \mu$ Fading Channels with Randomly Distributed Eavesdroppers", *2018 IEEE Intl. Conf. Commun. Workshops (ICC Workshops)*, pp. 1-6, May 20-24, 2018, Kansas City, USA.

- C3: **Kong L.**, Kaddoum G., Daniel Benevides da Costa, and Elias Bou-Harb, "On Secrecy Bounds of MIMO Wiretap Channels with ZF detectors", *2018 14th Intl. Wireless Commun. & Mobile Computing Conf. (IWCMC)*, Limassol, Jun. 25-29, 2018, pp. 724-729.

- C4: **Kong L.**, He J., Kaddoum G., Vuppala S., and Wang L., "Secrecy Analysis of A MIMO Full-Duplex Active Eavesdropper with Channel Estimation Errors", *2016 IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sept. 18-21, 2016, Montreal Canada.

- C5: Cai G., Wang L., **Kong L.** and Kaddoum G., "SNR Estimation for FM-DCSK System over Multipath Rayleigh Fading Channels", *2016 IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, Nanjing, 2016, pp. 1-5.

- C6: **Kong L.**, Kaddoum G., and Mostafa T., "Performance Analysis of Physical Layer Security of Chaos-based Modulation Schemes", *the Eighth IEEE intl. Workshop on Selected Topics in Wireless and Mobile computing (STWiMob)*, Abu Dhabi, UAE, Oct. 19-21, 2015.

- C7: Atallah M., Kaddoum G., and **Kong L.**, "A Survey of Cooperative Jamming Applied to Physical Layer Security", *IEEE intl. Conf. Ubiquitous Wireless Broadband (ICUWB)*, Montreal, Canada, Oct. 4-7, 2015.

LITERATURE REVIEW

The attempts of simply adding encryption schemes to the existing protocols at various communication layers, though provide security, come at the cost of additional computational complexity. Due to the limited storage capability and power constraints of light devices, the high computing-cost security techniques undoubtedly pose a heavy burden to communication devices (such as radio-frequency identification (RFID) tags, certain sensors, etc.) Poor, H. V. & Schaefer, R. F. (2017). Therefore, shifting the security to the physical layer can provide a promising solution. Physical layer security has emerged as an appealing and revolutionizing concept, which is not based on cryptography algorithms or secret keys (though they might support such solutions) Di Renzo, M. & Debbah, M. (2009); Duruturk, M. (2010); Shiu, Y. S., Chang, S. Y., Wu, H. C., Huang, S. C. H. & Chen, H. H. (2011). The foundation of physical layer security is information-theoretic, and it is supposed to be robust against attackers with any computing capabilities Jorswieck, E., Tomasin, S. & Sezgin, A. (2015).

1.1 State-of-the-arts of Physical Layer Security

1.1.1 Principle of Physical Layer Security

To illustrate the general concept of physical layer security, an example of a three-node wireless communication model is considered, as shown in Figure 1.1. In this network configuration, the sender node wishes to transmit its secret messages to the intended receiver node in the presence of a passive eavesdropper node. The communication link between the transmitter and the legitimate receiver is called the main channel, whereas the one between the transmitter and the eavesdropper is referred to as the wiretap channel. Usually the messages received in the legitimate and illegitimate terminals are different.

Wireless signals undergo many phenomena, including multipath fading, pathloss, etc. Fading is a self-interference physical phenomenon due to the multi-path propagation of the signals, while path-loss is indeed the attenuation of the wireless signal amplitude. It is mainly affected by the

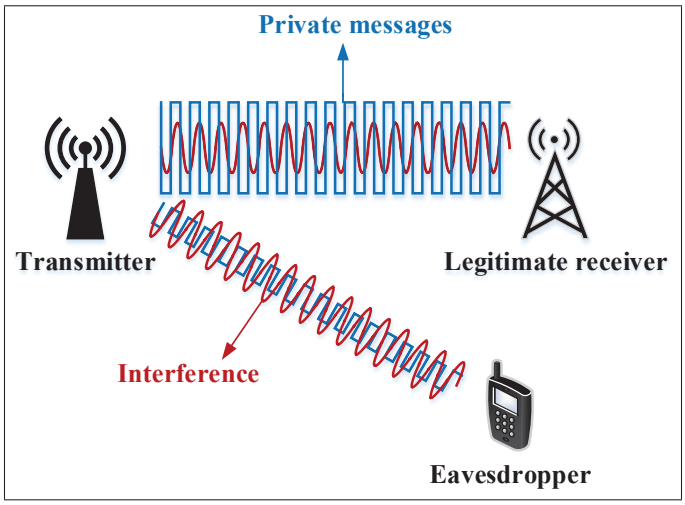


Figure 1.1 Illustration of wiretap channel model with one transmitter, one legitimate receiver and one eavesdropper

distance. In other words, if the legitimate users have information transmission over smaller distances, whereas the illegitimate users eavesdrop private information over wiretap channel with larger distance. Then, the received signal detected at legitimate users are certainly much strong than that at the eavesdroppers. In this vein, in wireless communication networks, the main objective of adopting physical-layer security is to maximize the rate of reliable information from the source to the legitimate destination, while all malicious nodes are kept as ignorant as possible of that information. The breakthrough philosophy behind physical-layer security is to exploit the characteristics of the wireless channel (i.e., fading, noise, interference) for achieving high reliability of wireless transmissions. While all these characteristics have traditionally been regarded as impairment factors for reliable communication, the paradigm of physical layer security takes advantage of these characteristics for achieving secure information transmission.

1.1.2 The Advantages of Physical Layer Security

The conceptual beauty of physical layer security is not only due to its essence of enhancing security at the bottom layer, but also to take advantage of the randomness of wireless links (i.e.,

noise, multipath fading, interference) as a feasible and effective means to address the security risks Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K. & Gao, X. (2018b).

As shown in Table 1.1, physical layer security is compared with the classical cryptography to list the pros and cons of these techniques.

Table 1.1 Comparisons between two techniques (Tech.) i.e., classical cryptography (CC) and physical layer security

Tech.	**Advantages**	**Disadvantages**
CC	1. Secret key based 2. Widely used in the upper layers and nearly every application of information and communication technology	1. Without information-theoretic security 2. High computing power 3. Low spectrum efficiency 4. One-way functions 5. Incapability of eavesdropping and interference in PHY layer
PLS	1. Information-theoretic based 2. No computational restrictions 3. Works at the bottom layer	1. Almost secure

1.1.3 The Evolution of Physical Layer Security over Fading Channels

On the way of prompting the research work on physical layer security, the following cornerstones are undoubtedly the fundamental masterpieces.

1) Shannon: the notion of information-theoretic secrecy was first introduced Shannon, C. (1949)

2) Wyner: the concept of wiretap channel model was established Wyner, A. D. (1975)

3) Csiszar and Korner: the existence of channel codes guaranteeing robustness to transmission errors was found Csiszar, I. & Korner, J. (1978)

4) Leung-Yan-Cheong and M. E. Hellman: Secrecy capacity over AWGN channel was mathematically expressed, which is the difference between the main channel capacity and the

wiretap channel capacity Leung-Yan-Cheong, S. & Hellman, M. (1978)

$$C_s = \log_2\left(1+\frac{P}{\delta_m}\right) - \log_2\left(1+\frac{P}{\delta_w}\right), \tag{1.1}$$

where P is the transmit power, δ_m, and δ_w are the noise variance at the legitimate user and eavesdroppers, respectively.

This work suggests that positive secrecy can be achieved, when the channel capacity for the AWGN wiretap channel is lower than that of the AWGN main channel. Consequently, confidential communication is impossible unless the Gaussian main channel has a better quality of received SNR than the Gaussian wiretap channel does.

5) Bolch *et al.*: Secrecy capacity over quasi-static fading channels was established Bloch, M., Barros, J., Rodrigues, M. R. D. & McLaughlin, S. W. (2008)

$$C_s = \left[\log_2\left(1+\underbrace{|h_m|^2\frac{P}{\delta_m}}_{\gamma_B}\right) - \log_2\left(1+\underbrace{|h_w|^2\frac{P}{\delta_w}}_{\gamma_E}\right)\right]^+, \tag{1.2}$$

where h_m and h_w are the channel fading coefficients of the legitimate channel and wiretap channel, respectively. γ_B and γ_E are used to represent the received instantaneous SNRs at the legitimate and illegitimate receivers, respectively.

The foundation laid by Bloch *et al.* demonstrates that in the presence of fading, information-theoretic security is achievable even when the eavesdropper has a better average SNR than the legitimate receiver (without the need for public communication over a feedback channel).

More recently, many researchers turned their attentions to the opportunistic exploitation of the space/time/user dimensions for secure communications. In Gopala, P. K., Lai, L. & Gamal, H. E. (2008), the secrecy capacity of ergodic slow fading channels was derived. The secrecy capacity of parallel fading channels was given in Liang, Y., Poor, H. & Shamai, S. (2008); Liu, T., Prabhakaran, V. & Vishwanath, S. (2008b), where Liang *et al.* (2008) considered the broad-

cast channel with a common message. Moreover, the secrecy capacity of the wiretap channel with multiple antennas was studied in Negi, R. & Goel, S. (2005),Parada, P. & Blahut, R. (2005),Khisti, A., Tchamkerten, A. & Wornell, G. W. (2008),Liu, T. & Shamai, S. (2009),Oggier, F. & Hassibi, B. (2011),Shafiee, S. & Ulukus, S. (2007). In particular, the secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel has been fully characterized in Khisti, A., Wornell, G., Wiesel, A. & Eldar, Y. (2007), Khisti, A. & Wornell, G. (2007), Liu & Shamai (2009), Oggier & Hassibi (2011) and more recently its closed-form expressions under a matrix covariance constraint have been derived in Bashar, S., Ding, Z. & Xiao, C. (2012). Furthermore, a large number of recent works have considered the secrecy capacity of more general broadcast channels. In Liu, R., Maric, I., Spasojevic', P. & Yates, R. (2008a), the authors study the two-user MIMO Gaussian broadcast channel. The two-user broadcast channel with two confidential messages, each of which must be kept secret to the unintended receiver, has been studied in Khisti, A. & Wornell, G. W. (2010a). A recent contribution has extended the result to the MIMO Gaussian broadcast channel Liu, R. & Poor, H. (2008). Multi-receiver wiretap channels have also been studied in Bagherikaram, G., Motahari, A. & Khandani, A. (2013); Choo, L.-C. & Wong, K.-K. (2009); Khisti *et al.* (2008) where the confidential messages to each receiver must be kept secret from an external eavesdropper.

The relay channel with confidential messages was studied in the works of Aggarwal, V., Sankar, L., Calderbank, A. & Poor, H. (2009); Lai, L. & Gamal, H. E. (2008); Oohama, Y. (2001,0). In this setup, one party communicates with another party directly, as well as through a relay node. In this work, the feedback channel was also studied because of its advantages over the wiretap channel. The general principle consists of two aspects: (1) when the main channel is noisier than the wiretap channel, feedback may permit unconditional secrecy; whereas without feedback this is not possible Leung-Yan-Cheong, S. K. (1976); (2) when the main channel and feedback channel are both noisy, perhaps it is possible to increase the secrecy capacity to the usual capacity without secrecy constraint Lai, L., El Gamal, H. & Poor, H. (2008); Tekin, E. & Yener, A. (2007). Finally, the role of feedback in multiple user channels was found to aid secrecy in Tang, X., Liu, R., Spasojevic, P. & Poor, H. (2007).

Since then, numerous researchers, from the fields of signal processing and wireless communications began to explore such an appealing paradigm for enhancing secrecy. The secrecy performance of point-to-point communication over AWGN, Rayleigh, Rician Kong, L. & Kaddoum, G. (2019), Nakagami-*m*, Weibull, $\alpha-\mu$ Kong, L., Tran, H. & Kaddoum, G. (2016b); Kong, L., Kaddoum, G. & da Costa, D. B. (2018a); Kong, L., Kaddoum, G. & Rezki, Z. (2018c), Fisher-Snedecor $\mathscr{F}$ Kong, L. & Kaddoum, G. (2018), and $\kappa-\mu/\eta-\mu$ fading channels Bloch *et al.* (2008); Kong *et al.* (2016b); Kumar, S., Chandrasekaran, G. & Kalyani, S. (2015); Liu, X. (2013a,1); Sarkar, M. Z. I., Ratnarajah, T. & Sellathurai, M. (2009) were investigated. Moreover, the secrecy performance of multiple-input single-output (MISO) systems, single-input multiple-output (SIMO) system, MIMO systems Kong, L., He, J., Kaddoum, G., Vuppala, S. & Wang, L. (2016a); Kong, L., Kaddoum, G., da Costa, D. B. & Bou-Harb, E. (2018b); Kong, L., Vuppala, S. & Kaddoum, G. (2018e), and MIMO multiple eavesdroppers (MIMOME) were fully characterized Khisti & Wornell (2010a); Khisti *et al.* (2007); Oggier & Hassibi (2011).

With the recent emergence of various communication networks and technologies, there has been a growing research interest in the applications of physical layer secrecy techniques for various wireless systems, such as mmWave communications Vuppala, S., Tolossa, Y. J., Kaddoum, G. & Abreu, G. (2018); Wang, C. & Wang, H. M. (2016), cooperative networks Wang, C., Wang, H., Ng, D. W. K., Xia, X. & Liu, C. (2015a); Yao, J., Zhou, X., Liu, Y. & Feng, S. (2018); Zhang, N., Cheng, N., Lu, N., Zhang, X., Mark, J. & Shen, X. (2015b), cognitive radios networks Kwon, T., Wong, V. & Schober, R. (2012); Wang, C. & Wang, H.-M. (2014), orthogonal frequency-division multiplexing (OFDM) systems Zhang, H., Xing, H., Cheng, J., Nallanathan, A. & Leung, V. C. M. (2016a); Zhang, M. & Liu, Y. (2016), wireless ad hoc and multi-hop networks and cellular networks (LTE, 5th Generation (5G) Yang *et al.* (2015), Massive MIMO Kapetanovic, D., Zheng, G. & Rusek, F. (2015)), satellite communications Lin, M., Lin, Z., Zhu, W. & Wang, J. (2018); Zheng, G., Arapoglou, P. & Ottersten, B. (2012), internet of things Mukherjee, A. (2015) , wireless body area networks (WBAN) Moosavi & Bui (2016), Smart Grid Lee, E.-K., Gerla, M. & Oh, S. (2012), wireless sensor networks (WSNs)

Jameel, F., Wyne, S. & Krikidis, I. (2017); Zou, Y. & Wang, G. (2016), devices-to-devices (D2D) communications Tolossa, Y. J., Vuppala, S., Kaddoum, G. & Abreu, G. (2018); Wang, L., Liu, J., Chen, M., Gui, G. & Sari, H. (2018), ultra-dense networks Kamel, M., Hamouda, W. & Youssef, A. (2017), visible light communication Pan, G., Ye, J. & Ding, Z. (2017), NOMA Tran, D., Tran, H., Ha, D. & Kaddoum, G. (2019), *etc*.

1.1.4 Secrecy Metrics

According to Bloch *et al.* (2008), the instantaneous secrecy capacity over fading channels is defined as the difference between the main channel capacity $C_M = \log_2(1+\gamma_B)$ and the wiretap channel capacity $C_W = \log_2(1+\gamma_E)$,

$$C_s = \begin{cases} C_M - C_W, & \gamma_B > \gamma_E \\ 0, & \text{otherwise}, \end{cases} \tag{1.3}$$

where γ_B and γ_E are the received SNRs at the legitimate and illegitimate receivers, respectively.

1.1.4.1 Secrecy Outage Probability

The outage probability of the secrecy capacity is defined as the probability that the secrecy capacity C_s falls below the target secrecy rate R_s, i.e.,

$$P_{out}(R_s) = Pr(C_s < R_s). \tag{1.4}$$

The secrecy outage probability can be conceptually explained by two cases: (i) the instantaneous secrecy capacity C_s is lower than the given target secrecy transmission rate, even though positive secrecy capacity is guaranteed; (ii) secrecy outage event definitely happens when the

secrecy capacity is non-positive. Thus, (1.4) can be mathematically rewritten as

$$\begin{aligned} P_{out}(R_s) &= Pr(C_s < R_s | \gamma_B > \gamma_E) Pr(\gamma_B > \gamma_E) + Pr(\gamma_B < \gamma_E) \\ &= \int_0^{\infty} \int_{\gamma_E}^{\gamma_0} f_B(\gamma_B) f_E(\gamma_E) d\gamma_B d\gamma_E + \int_0^{\infty} \int_0^{\gamma_E} f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_B d\gamma_E \\ &= \int_0^{\infty} f_{\gamma_E}(\gamma_E) \left[\int_0^{\gamma_0} - \int_0^{\gamma_E} \right] f_{\gamma_B}(\gamma_B) d\gamma_B d\gamma_E + \int_0^{\infty} \int_0^{\gamma_E} f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_B d\gamma_E \\ &= \int_0^{\infty} F_{\gamma_B}(\gamma_0) f_{\gamma_E}(\gamma_E) d\gamma_E, \end{aligned} \tag{1.5}$$

where $\gamma_0 = M(1+\gamma_E) - 1$, $M = 2^{R_s}$. F_B and F_E are used to denote the CDFs of the received instantaneous SNRs at Bob and Eve, respectively. Similarly, f_B and f_E are utilized to express the PDFs of the received instantaneous SNRs at Bob and Eve, respectively.

1.1.4.2 The probability of non-zero secrecy capacity

The probability of non-zero secrecy capacity refers to an event that the positive secrecy capacity can be achieved, i.e. $Pr(C_s > 0)$. With regards to this definition, the PNZ is further rewritten as

$$\begin{aligned} Pr(C_s > 0) &= Pr(\gamma_B > \gamma_E) \\ &= \int_0^{\infty} \int_0^{\gamma_B} f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_E d\gamma_B \\ &= \int_0^{\infty} f_{\gamma_B}(\gamma_B) F_{\gamma_E}(\gamma_B) d\gamma_B. \end{aligned} \tag{1.6}$$

1.1.4.3 Average secrecy capacity

The secrecy capacity undoubtedly plays a vital role in physical layer security. It is a significant benchmark to measure the fundamental limit of the secure transmission between different parties over noisy and fading channels. It is theoretically associated with Wyner's wiretap channel model. For the sake of providing a simple form of calculating the average secrecy capacity $\bar{C}_s$, the following expression is given Lei, H., Ansari, I. S., Pan, G., Alomair, B. & Alouini, M. S.

(2017a).

$$\begin{aligned}\bar{C}_s = &\underbrace{\int_0^\infty \log_2(1+\gamma_B) f_B(\gamma_B) F_E(\gamma_B) d\gamma_B}_{I_1} + \underbrace{\int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) F_B(\gamma_E) d\gamma_E}_{I_2} \\ &- \underbrace{\int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) d\gamma_E}_{I_3}.\end{aligned} \tag{1.7}$$

1.2 Wireless Fading Channels

One of the main contributions of this dissertation is to consider more general and flexible fading channels. In this subsection, three key fading channels are listed.

1.2.1 $\alpha-\mu$ Fading Channels

The $\alpha-\mu$ distribution was first proposed by Yacoub in 2007 Yacoub, M. D. (2007a). Its PDF is given w.r.t. X as follows

$$f_X(x) = \frac{\alpha \mu^\mu x^{\alpha\mu-1}}{\hat{\Omega}^{\alpha\mu}\Gamma(\mu)} \exp\left(-\mu\left(\frac{x}{\hat{\Omega}}\right)^\alpha\right), \tag{1.8}$$

where $\Omega = \sqrt[\alpha]{E\left(x^\alpha\right)}$ is the $\alpha-$root mean value, $\alpha > 0$ is an arbitrary fading parameter used to denote the non-linearity of environments. $\mu > 0$ is the inverse of the normalized variance of x^α, which is used to denote the number of multipath clusters. The parameter μ is calculated by $\mu = \frac{\mathscr{E}^2(x^\alpha)}{\mathscr{V}(x^\alpha)}$.

The CDF of $\alpha-\mu$ distribution is given by

$$F_X(x) = \frac{\Gamma\left(\mu, \mu\left(\frac{x}{\hat{\Omega}}\right)^\alpha\right)}{\Gamma(\mu)}. \tag{1.9}$$

The general $\alpha - \mu$ fading distribution can be reduced to several well-known fading models. For example,

- when $\alpha = 2, \mu = 1$, the Rayleigh distribution is obtained;
- when $\alpha = 2, \mu = m$, it is then reduced to the Nakagami-m distribution;
- when α is the fading parameter, and $\mu = 1$, it is the so-called Weibull distribution.

Later on, it has been reported in the literature that, in the filed experiments, the $\alpha - \mu$ distribution characterizes several different wireless communication scenarios Chong *et al.* (2011); Dias, U. S. & Yacoub, M. D. (2009); Karadimas, P., Vagenas, E. D. & Kotsopoulos, S. A. (2010); Michalopoulou, A., Zervos, T., Peppas, K., Lazarakis, F., Alexandridis, A. A., Dangakis, K. & Kaklamani, D. I. (2011); Michalopoulou, A., Alexandridis, A. A., Peppas, K., Zervos, T., Lazarakis, F., Dangakis, K. & Kaklamani, D. I. (2012); Reig, J. & Rubio, L. (2013); Wu *et al.* (2010), including V2V communication networks and WBAN.

1.2.2 Fisher-Snedecor $\mathscr{F}$ Fading Channels

The Fisher-Snedecor $\mathscr{F}$ distribution was first proposed by Yoo *et.al* in 2017 to characterize device-to-device (D2D) communication links. Compared to the other frequently used channel model, i.e., the generalized-K distribution, the Fisher-Snedecor $\mathscr{F}$ is experimentally studied and proved with a good, and in most cases, a better fit to the real channel data. This distribution demonstrates a simple but effective fading model, especially at 5.8GHz for both indoor and outdoor environments.

Technically speaking, the Fisher-Snedecor $\mathscr{F}$ distribution is modeled with two parameters, i.e., m and m_s. m and m_s represent the amount of shadowing of the root-mean-square (rms) signal power and the fading severity parameter, respectively. The PDF and CDF of the Fisher-Snedecor $\mathscr{F}$ distribution are respectively given by

$$f_X(x) = \frac{2m^m (m_s\Omega)^{m_s} x^{2m-1}}{\mathscr{B}(m, m_s)(mx^2 + m_s\Omega)^{m+m_s}}, \tag{1.10}$$

$$F_X(x) = \frac{m^{m-1}x^{2m}{}_2F_1\left(m+m_s, m; m+1; -\frac{mx^2}{m_s\Omega}\right)}{\mathscr{B}(m,m_s)(m_s\Omega)^m}, \tag{1.11}$$

where $\mathscr{B}(m,m_s)$ is the beta function, $\Omega = \mathscr{E}[x^2]$ is the mean power.

In addition, it is worthy to mention that Fisher-Snedecor $\mathscr{F}$ distribution is also flexible since it can be attributed to some other fading models by fixing m and m_s with special values. For example, when $m_s \to \infty$, and $m = m$, it is Nakagami-m distribution. Further for $m = 1$, it is the Rayleigh distribution.

1.2.3 Fox's H-function Fading Channels

The Fox's H-function distribution was introduced as a pure mathematical finding by Cook in 1981 Cook Jr, I. D. (1981). It is much more flexible since it can be easily generalized to many fading models, such as Gamma, exponential, Chi-square, Weibull, Rayleigh, Half-normal, as well as the two aforementioned fading models.

The Fox's H-function distribution is much more flexible and generic, due to its mathematical definition, which is given by

$$\begin{aligned} f_X(x) &= \kappa H_{p,q}^{m,n}\left[\lambda x \left| \begin{matrix}(a_i,A_i)_{i=1:p}\\(b_l,B_l)_{l=1:q}\end{matrix}\right.\right], \quad \gamma > 0, \\ &\overset{(a)}{=} \frac{\kappa}{2\pi j}\int_{\mathscr{L}} \underbrace{\frac{\prod_{i=1}^{m}\Gamma(b_l+B_ls)\prod_{l=1}^{n}\Gamma(1-a_i-A_is)}{\prod_{i=m+1}^{q}\Gamma(1-b_l-B_ls)\prod_{l=n+1}^{p}\Gamma(a_i+A_is)}}_{\Theta(s)}(\lambda x)^{-s}ds, \end{aligned} \tag{1.12}$$

where $\lambda > 0$ and κ are constants such that $\int_0^\infty f_k(\gamma_k)d\gamma_k = 1$. $j = \sqrt{-1}$, $(x_i,y_i)_l$ is a shorthand for $(x_1,y_1),\cdots,(x_l,y_l)$. Step (a) is developed by expressing Fox's H-function in terms of its definition (Mathai, A. M., Saxena, R. K. & Haubold, H. J., 2009a, eq. (1.2)). $A_i > 0$ for all $i = 1,\cdots,p$, and $B_l > 0$ for all $l = 1,\cdots,q$. $0 \le m \le q$, $0 \le n \le p$, $\mathscr{L}$ is a suitable contour

separating the poles of the gamma functions $\Gamma(b_l + B_l s)$ from the poles of the gamma functions $\Gamma(1 - a_i - A_i s)$.

As reported in the literature, the Fox's H-function distribution provides a general but feasible model that compasses most distributions. This is due to its property to re-express those functions in the form of Fox's H-function Bodenschatz, C. D. (1992). For instance, Rayleigh distribution includes exponential function and power functions. By using 1.13, Rayleigh distribution is then the so-called Fox's H-function distribution.

For the purposes of showing the effectiveness and feasibility of Fox's H-function distribution, we have listed several special functions, which can be transformed in terms of the Fox's H-function Prudnikov, A. P., Brychkov, Y. A. & Marichev, O. I. (1990).

$$\frac{1}{B}x^{\frac{b}{B}}\exp\left(-x^{\frac{1}{B}}\right) = H_{0,1}^{1,0}\left[x\left|\begin{array}{c} - \\ (b,B) \end{array}\right.\right], \tag{1.13}$$

$$\ln(1+x) = H_{2,2}^{1,2}\left[x\left|\begin{array}{c} (1,1),(1,1) \\ (1,1),(0,1) \end{array}\right.\right], \tag{1.14}$$

$$\Gamma(a,x) = H_{1,2}^{2,0}\left[x\left|\begin{array}{c} (1,1) \\ (0,1),(a,1) \end{array}\right.\right]. \tag{1.15}$$

1.3 Fox's H-function

The Fox's H-function is a general function involving Mellin-Barnes integrals Mathai *et al.* (2009a). It is a generalization of Meijer's G-function. In this dissertation, both the univariate and bivariate Fox's H-functions play an important role when deriving the secrecy metrics. As such, this subsection offers a brief introduction of these two functions.

1.3.1 The Univariate Fox's H-function

Without the constraints of λ and κ, i.e., $\lambda > 0$, and κ is constant, the univariate Fox's H-function is defined as follows

$$H_{p,q}^{m,n}\left[x\left|\begin{array}{l}(a_i,A_i)_{i=1:p}\\(b_l,B_l)_{l=1:q}\end{array}\right.\right]=\frac{1}{2\pi j}\int_{\mathscr{L}}\Theta(s)x^{-s}ds. \tag{1.16}$$

The Meijer's G-function is a special case of Fox's H-function obtained by simply setting all $A_i = 1, i = 1,\cdots,p$ and $B_l = 1, l = 1,\cdots,q$. In other words,

$$H_{p,q}^{m,n}\left[x\left|\begin{array}{l}(a_i,A_i)_{i=1:p}\\(b_l,B_l)_{l=1:q}\end{array}\right.\right]=G_{p,q}^{m,n}\left[x\left|\begin{array}{l}(a_i)_{i=1:p}\\(b_l)_{l=1:q}\end{array}\right.\right]. \tag{1.17}$$

1.3.2 The Bivariate Fox's H-function

Similarly, the bivariate Fox's H-function is defined as follows Mathai, A. M. & Saxena, R. K. (1978):

$$\begin{aligned}&H_{p,q;p_1,q_1;p_2,q_2}^{m,n;m_1,n_1;m_2,n_2}\left[x,y\left|\begin{array}{l|l|l}(a_i;\alpha_i,A_i)_{i=1:q} & (c_i,C_i)_{i=1:q_1} & (e_i,E_i)_{i=1:q_2}\\(b_l;\beta_l,B_l)_{l=1:p} & (d_l,D_l)_{l=1:p_1} & (f_l,F_l)_{l=1:p_2}\end{array}\right.\right]\\&=-\frac{1}{4\pi^2}\int_{\mathscr{L}_1}\int_{\mathscr{L}_2}\Theta(s,\xi)\Theta(\xi)\Theta_E(s)x^{\xi}y^s dsd\xi,\end{aligned} \tag{1.18}$$

where $\mathscr{L}_1$ and $\mathscr{L}_2$ are two suitable contours, $m,n,m_1,n_1,m_2,n_2,p,q,p_1,q_1,p_2,q_2$ are positive integers with constraints: $0 \le m \le q$, $0 \le n \le p$, $0 \le m_1 \le q_1$, $0 \le n_1 \le p_1$, $0 \le m_2 \le q_2$, $0 \le n_2 \le p_2$. The sequence of parameters α_q, β_p, A_q, B_p, C_{q_1}, D_{p_1}, E_{q_2}, and F_{p_2} are real and positive numbers.

$$\Theta(s,\xi)=\frac{\prod_{i=1}^{n_1}\Gamma(1-a_i+\alpha_i s+A_i\xi)\prod_{l=1}^{m_1}\Gamma(b_l-\beta_l s-B_l\xi)}{\prod_{i=n_1+1}^{p_1}\Gamma(a_i-A_i s-A_i\xi)\prod_{l=m_1+1}^{q_1}\Gamma(1-b_l+B_l s+B_l\xi)}, \tag{1.19a}$$

$$\Theta(\xi) = \frac{\prod_{i=1}^{m_1} \Gamma(d_l - D_l\xi) \prod_{l=1}^{n_1} \Gamma(1 - c_i + A_i\xi)}{\prod_{i=m_1+1}^{q_1} \Gamma(1 - d_l + D_l\xi) \prod_{l=n_1+1}^{p_1} \Gamma(d_i - D_i\xi)}, \tag{1.19b}$$

$$\Theta(s) = \frac{\prod_{i=1}^{m_1} \Gamma(f_l - F_l s) \prod_{l=1}^{n_1} \Gamma(1 - e_i + E_i s)}{\prod_{i=m_1+1}^{q_1} \Gamma(1 - f_l + F_l s) \prod_{l=n_1+1}^{p_1} \Gamma(e_i - E_i s)}. \tag{1.19c}$$

In addition, on condition that $C_i = 1$, $D_l = 1$, $E_i = 1$, and $F_l = 1$, the bivariate Fox's H-function is reduced to the bivariate Meijer's G-function. The univariate and bivariate Meijer's G-functions are thereafter used in Chapters 4, 5, 6, and 7.

CHAPTER 2

PERFORMANCE ANALYSIS OF PHYSICAL LAYER SECURITY OVER $\alpha - \mu$ FADING CHANNEL

Long Kong, Hung Tran, and Georges Kaddoum

Département de Génie électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper published in *IET Electronics Letters*, January 2016.

2.1 Abstract

Recently, many works have focused on analyzing the metrics of physical layer security over different wireless channels, such as additive white Gaussian noise (AWGN), Rayleigh, Rician and Nakagami-*m* fading distributions. In order to extend the analysis to the general case, $\alpha - \mu$ fading channel is considered, which can span the aforementioned cases. For this purpose, the physical layer security over $\alpha - \mu$ fading channel is presented in this letter. The closed-form expressions for the probability of positive secrecy capacity and upper bound of the secrecy outage probability are derived. Their accuracies are assessed through comparison of theoretical analysis and simulations results.

2.2 Introduction

Physical layer security is a promising solution that addresses the security issue while directly operating at the physical layer from the information-theoretic viewpoint. Numerous contributions exist that analyze the secrecy performance over AWGN, Rayleigh, Rician, Nakagam-*m* and Weibull fading channels. Performance analysis in terms of secrecy capacity and outage probability has been investigated Bloch *et al.* (2008); Liu (2013a,1); Sarkar *et al.* (2009). However, to the best knowledge of the authors, there is no previous work focusing on the general case of fading channels. With regard to different values of α and μ, the $\alpha - \mu$ fading channel can be reduced to the specific fading channel, such as Rayleigh, Nakagami-*m* and Weibull fad-

ing distributions by adjusting certain parameters. In this letter, the secrecy performance over $\alpha - \mu$ fading channel is evaluated by the closed-form expressions for the probability of positive secrecy capacity and upper bound of secrecy outage probability. Consequently, our theoretical analysis is confirmed by simulation results.

2.3 System model and secrecy performance analysis

A three-node classic model such as the one shown in Fig. 2.1 is used here to illustrate a wireless network with potential eavesdropping. In the wiretap channel model, a legitimate transmitter (Alice) equipped with a directional antenna wishes to send secret messages to an intended receiver (Bob) in the presence of an eavesdropper (Eve), the link between Alice and Bob with fading coefficient h_m is called the main channel, while the one between Alice and Eve with fading coefficient h_w is named as the wiretap channel. Both channels undergo the $\alpha - \mu$ distribution.

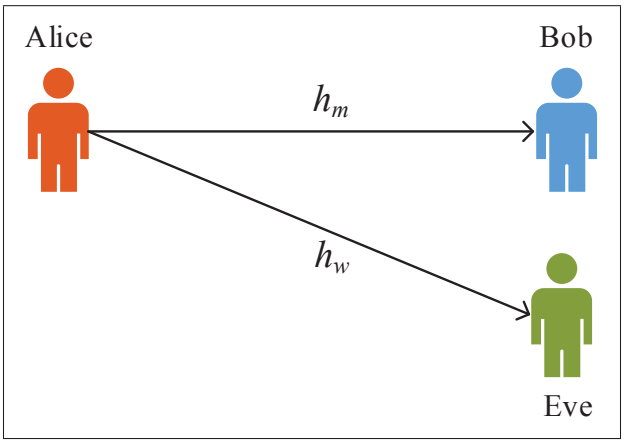


Figure 2.1 Illustration of system model with two legitimate transceivers (Alice and Bob) and one eavesdropper (Eve)

Recalling that the probability density function (PDF) of the $\alpha-\mu$ fading channel coefficients $h_i, (i \in \{m, w\})$ is given by Yacoub (2007a)

$$f_{h_i}(h) = \frac{\alpha_i \mu_i^{\mu_i} h^{\alpha_i \mu_i - 1}}{\hat{h}_i^{\alpha_i \mu_i} \Gamma(\mu_i)} \exp\left(-\mu_i \frac{h^{\alpha_i}}{\hat{h}_i^{\alpha_i}}\right), \tag{2.1}$$

where $\hat{h}_i = \sqrt[\alpha]{E\left(h_i^{\alpha_i}\right)}$ is the $\alpha-$root mean value, $\alpha_i > 0$ is an arbitrary fading parameter, $\mu_i > 0$ is the inverse of the normalized variance of $h_i^{\alpha_i}$. The parameter μ_i is calculated by $\mu_i = E^2\left(h_i^{\alpha_i}\right)/V\left(h_i^{\alpha_i}\right)$, where $E(\cdot)$ and $V(\cdot)$ are the expectation and variance operators, respectively. $\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} dt$ is the Euler's Gamma function. In particular, when changing the values of α and μ to the following cases: (i) $\alpha = 2$, $\mu = 1$; (ii) $\alpha = 2$, $\mu = m$; and (iii) $\mu = 1$, the α-μ fading model can be simplified such that it follows Rayleigh, Nakagami-m and Weibull distributions, respectively.

Let $g_i = |h_i|^2$ denote the instantaneous channel power gain with unit mean. The PDF of g_i is expressed as Song, Y., Shin, H. & Kim, W. (2008)

$$f_{g_i}(x) = \frac{\alpha_i x^{\frac{\alpha_i \mu_i}{2} - 1}}{2\Omega_i^{\frac{\alpha_i \mu_i}{2}} \Gamma(\mu_i)} \exp\left[-\left(\frac{x}{\Omega_i}\right)^{\frac{\alpha_i}{2}}\right], \tag{2.2}$$

where $\Omega_i = \frac{\Gamma(\mu_i)}{\Gamma(\mu_i + \frac{2}{\alpha_i})}$. Therefore, the received signal-to-noise ratio (SNR) at Bob and Eve receiver sides can be expressed as

$$\gamma_i = \frac{P_i g_i}{N_i} \tag{2.3}$$

where P_i and N_i are the transmission power and noise power, respectively. Without loss of generality, we assume N_m is equal to N_w in this paper. In addition, since we consider that Alice is equipped with a directional antenna, then the transmitted powers P_m and P_w may be different because Bob and Eve are present in different locations in the network.

According to Bloch *et al.* (2008); Liu (2013a,1); Sarkar *et al.* (2009), the secrecy capacity for the given network is given as follows

$$C_s = C_m - C_w = \begin{cases} \log_2\left(\frac{1+\gamma_m}{1+\gamma_w}\right), & \text{if } \gamma_m > \gamma_w \\ 0, & \text{if } \gamma_m \leqslant \gamma_w \end{cases} \tag{2.4}$$

where C_m and C_w are the capacities of the main channel and the wiretap channel, respectively.

Therefore, the probability of positive secrecy capacity can be derived as follows

$$\begin{aligned} Pr\left(C_s > 0\right) &= Pr\left[\log_2\left(\frac{1+\gamma_m}{1+\gamma_w}\right) > 0\right] \\ &= Pr\left(\gamma_m > \gamma_w\right) \\ &= 1 - Pr\left(\frac{\gamma_m}{\gamma_w} < 1\right) \\ &= 1 - Pr\left(\frac{g_m}{g_w} < \frac{P_w}{P_m}\right). \end{aligned} \tag{2.5}$$

According to equation (16) in Tran, H., Duong, T. Q. & Zepernick, H. (2011), equation (2.5) is derived as

$$Pr\left(C_s > 0\right) = 1 - F_\gamma(1) \tag{2.6}$$

where $F_\gamma(x)$ is the cumulative distribution function (CDF) of x, which is given as

$$\begin{aligned} F_\gamma(x) &= Pr\left(\frac{g_m}{g_w} < \frac{P_w}{P_m} \cdot x\right) \\ &= \left(\frac{P_w\Omega_w}{P_m\Omega_m}\right)^{\frac{\alpha\mu_m}{2}} \frac{x^{\frac{\alpha\mu_m}{2}}}{\mu_m \beta\left(\mu_m, \mu_w\right)} {}_2F_1\left(\mu_m + \mu_w, \mu_m; 1+\mu_m; -\left(\frac{P_w\Omega_w}{P_m\Omega_m}\right)^{\frac{\alpha}{2}} x^{\frac{\alpha}{2}}\right), \end{aligned} \tag{2.7}$$

herein ${}_2F_1\left(.,;.;.\right)$ denotes the Gaussian hypergeometric function and $\beta(.,.)$ is the Beta function.

The outage probability of the secrecy capacity is defined as the probability that the secrecy capacity C_s falls below the target secrecy rate R_s, i.e.

$$\begin{aligned} P_{out}\left(C_s \leqslant R_s\right) &= Pr\left[\log_2\left(\frac{1+\gamma_m}{1+\gamma_w}\right) \leqslant R_s\right] \\ &= Pr\left[\gamma_m \leqslant 2^{R_s}\left(1+\gamma_w\right)-1\right] \\ &= Pr\left(\gamma_m \leqslant \gamma_{th}+\gamma_{th}\gamma_w-1\right), \end{aligned} \tag{2.8}$$

where $\gamma_{th} = 2^{R_s}$. Due to the complex form of the PDF of α-μ fading distribution, it is difficult to obtain a closed-form expression for (2.8). However, when the target data rate R_s approaches zero, we can obtain the upper bound of the outage probability by substituting equation (2.7) into equation (2.8), to get the following relationship

$$\begin{aligned} P_{out}\left(C_s \leqslant R_s\right) &= Pr\left(\gamma_m \leqslant \gamma_{th}+\gamma_{th}\gamma_w-1\right) \\ &\leqslant Pr\left(\gamma_m \leqslant \gamma_{th}\gamma_w\right) \\ &\leqslant Pr\left(\frac{\gamma_m}{\gamma_w} \leqslant \gamma_{th}\right) \\ &\leqslant Pr\left(\frac{g_m}{g_w} \leqslant \frac{P_w}{P_m}\cdot\gamma_{th}\right) \\ &\leqslant F_\gamma\left(\gamma_{th}\right). \end{aligned} \tag{2.9}$$

2.4 Numerical Analysis

Fig. 2.2 shows the simulation and analysis results of the probability of positive secrecy capacity versus the transmission power P_m over $\alpha-\mu$ fading channel for selected power values of eavesdropper P_w provided that $\alpha = 2$ and $\mu_m = \mu_w = 1$ (Rayleigh fading). One can observe that the analytical and simulation results are in perfect match for any given set of parameters. In addition, for the case of fixed values of P_w, the larger P_m the higher the probability of positive secrecy capacity. In Fig. 2.3, the probability of positive secrecy capacity in terms of different values of α and μ for fixed $P_w = 10$ dB is illustrated. Here, a similar conclusion is obtained to that of Fig. 2.2.

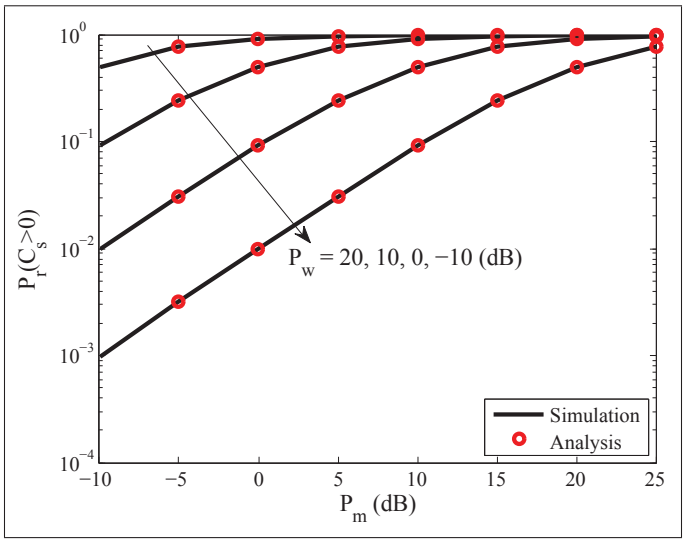


Figure 2.2 The probability of positive secrecy capacity versus P_m for selected values of P_w values with fixed values of $\alpha = 2$ and $\mu_m = \mu_w = 1$

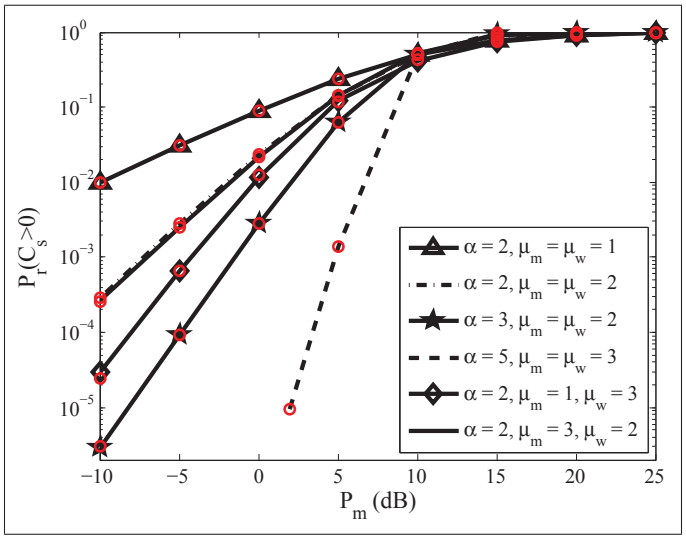


Figure 2.3 The probability of positive secrecy capacity versus P_m for different values of α and μ_i and a fixed value of $P_w = 10$ dB. The solid and circle (o) lines correspond to the simulation and analysis results, respectively

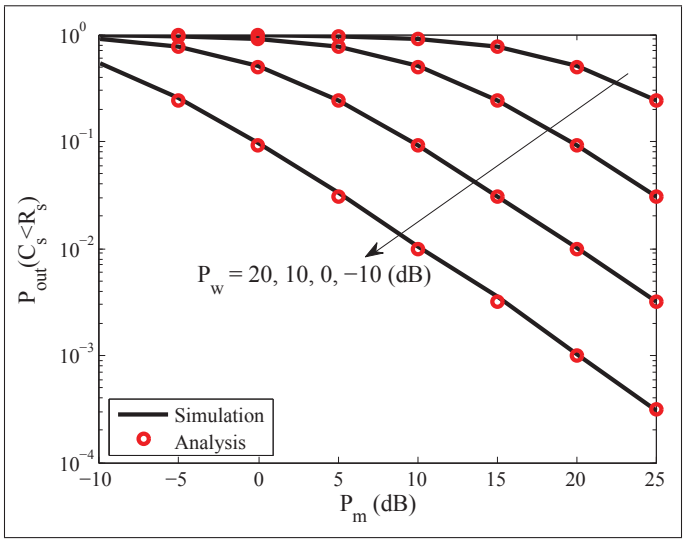


Figure 2.4 The upper bound of secrecy outage probability versus P_m for selected values of P_w with fixed values of $\alpha = 2$ and $\mu_m = \mu_w = 1$

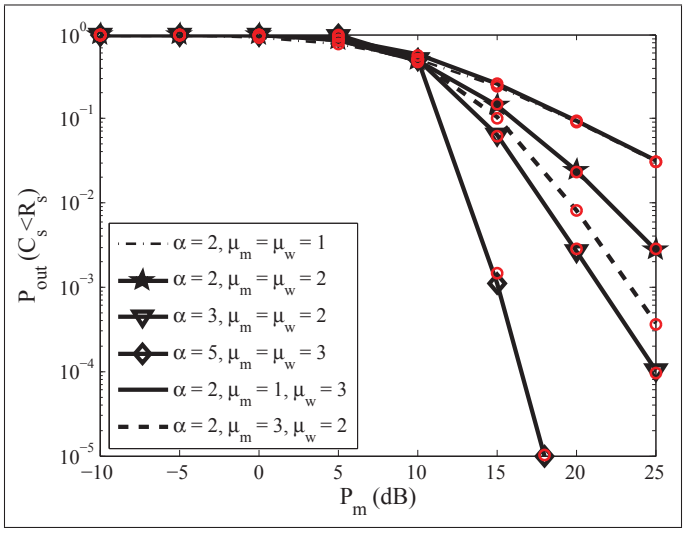


Figure 2.5 The upper bound of secrecy outage probability versus P_m for different values of α and μ_i and a fixed value of $P_w = 10$ dB. The solid and circle (o) lines correspond to simulation and analysis results, respectively

Similarly, Fig. 2.4 and Fig. 2.5 show the simulation and analysis results of the upper bound of the outage probability of physical layer security over $\alpha-\mu$ fading channel with regard to two cases: (i) fixed $\alpha=2$, $\mu_m=\mu_w=1$ while varying P_w; (ii) fixed P_w while changing the values of α and μ. Here, we fix the target data rate as $R_s=0.01$ bps. We can easily draw the same conclusion about the accuracy of our derived expression for the upper bound of outage probability, i.e. analytical derivations are verified by the simulation results.

2.5 Conclusion

In this letter, we derive closed-form expressions for the probability of positive secrecy capacity and upper bound of outage probability for physical layer security over $\alpha-\mu$ fading channels. For verification and correctness measures, the derived closed-form expressions are validated by simulation results.

CHAPTER 3

HIGHLY ACCURATE AND ASYMPTOTIC ANALYSIS ON THE SOP OVER SIMO $\alpha-\mu$ FADING CHANNELS

Long Kong[1], Georges Kaddoum[1], and Zouheir Rezki[2]

[1]Département de Génie électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3
[2]Electrical and Computer Engineering Department, University of Idaho, Moscow, ID, USA.

Paper published in *IEEE Communications Letters*, July 2018.

3.1 Abstract

In order to fill the gap of the mathematical analysis's lack for the secrecy outage probability (SOP) over single-input multiple-output (SIMO) $\alpha-\mu$ wiretap fading channels, this letter initially provides highly accurate and asymptotic closed-form expressions for the SOP. The novel highly accurate formulations are derived in a *simple* and *general* form in terms of the bivariate Fox's H-function, which is extensively used in the literature. Additionally, the asymptotic analysis of the SOP is derived at high signal-to-noise ratio (SNR) regime. The obtained expressions are numerically validated and compared with the Monte-Carlo simulation results. The derived SOP is in highly accurate match with simulation results for SIMO case, and perfect match with simulated results for single-input single-output (SISO) case.

Keywords: SIMO $\alpha-\mu$ wiretap fading channels, secrecy outage probability, asymptotic analysis, Fox's H-function.

3.2 Introduction

Physical layer security (PLS) readily sharpens our vision and subsequently enjoys great appetite of the academia and industrial spheres, responding to the inherent open nature of wireless transmission medium. The initial theoretical works for the PLS have laid solid foundations to address security issues from the information theoretical perspective. Later on, many aspects

of PLS began with the secrecy analysis over additive white Gaussian noise (AWGN)Leung-Yan-Cheong & Hellman (1978) channel, and afterwards shifted to that over various fading channels, such as Rayleigh Bloch *et al.* (2008), Nakagami-*m* Sarkar *et al.* (2009), Weibull Liu (2013b), and $\alpha-\mu$ (equivalently, generalized Gamma) Kong *et al.* (2016b); Lei, H., Gao, C., Guo, Y. & Pan, G. (2015); Lei *et al.* (2017a), etc., wiretap fading channels.

On the other hand, the $\alpha-\mu$ fading model encompasses Rayleigh, Nakagami-*m*, Exponential and Weibull fading Yacoub (2007a), and resultantly, the characterization of secrecy analysis over $\alpha-\mu$ wiretap fading channels is decisively significant. Revisiting all existing results concerning the secrecy performance over $\alpha-\mu$ wiretap channels Kong *et al.* (2016b); Lei *et al.* (2015,1), the works either focused on deriving the average secrecy capacity (ASC) Lei *et al.* (2017a), the probability of non-zero secrecy capacity (PNZ) Kong *et al.* (2016b), or a lower bound of the secrecy outage probability (SOP) Lei *et al.* (2015). It is worthy to note that the analytical expressions of the ASC and lower bound of the SOP were respectively provided with respect to the bivariate Fox's *H*-function and Meijer's *G*-function in Lei *et al.* (2015,1).

In fact, the difficulty to obtain closed-form expressions, for the corresponding intractable integrals, explicitly leads to the derivation of a lower bound on the SOP. Apart from the analysis on the lower bound, none of them presents an exact closed-form expressions for the SOP, let alone its extension to the single-input multiple-output (SIMO) scenario.

To fill this gap, the objective thereafter is to complete the secrecy investigation over the SIMO $\alpha-\mu$ wiretap fading channels. More specifically, the contributions of this paper are as follows:

- Providing an exact SOP expression for single-input multiple-output (SISO) $\alpha-\mu$ wiretap fading channels.
- Considering the sum of multiple $\alpha-\mu$ random variables (RVs) as another $\alpha-\mu$ distributed RV da Costa, D. B., Yacoub, M. D. & Filho, J. C. S. S. (2008); Zhang, J., Dai, L., Wang, Z., Ng, D. W. K. & Gerstacker, W. H. (2015a), and deriving highly accurate SOP and lower bound of SOP over SIMO $\alpha-\mu$ wiretap fading channels.

- Benefiting from the derived analytical SOP expression, we provide asymptotic analysis of the SOP and secrecy diversity order, especially at high signal-to-noise ratio (SNR) regime, due to the non-elementary form of the derived SOP.

Notations: $[x]^+ = \max(x,0)$. $\Gamma(.)$ is the complete Gamma function (Gradshteyn, I. S. & Ryzhik, I. M., 2014, Eq. (8.310.1)), $\Gamma(a,x)$ is the upper incomplete Gamma function (Gradshteyn & Ryzhik, 2014, Eq. (8.350.2)). $H_{p,q}^{m,n}[.]$ is the univariate Fox's H-function (Mathai *et al.*, 2009a, Eq. (1.2)), $H_{p,q:p_1,q_1:p_2,q_2}^{0,n:m_1,n_1:m_2,n_2}$ is the bivariate Fox's H-function (Mathai *et al.*, 2009a, Eq. (2.56)). $\mathscr{B}(x,y)$ is the Beta function (Gradshteyn & Ryzhik, 2014, Eq. (8.380.1)). $\mathscr{M}[f(x),s]$ denotes the Mellin transform of $f(x)$ (Debnath, L. & Bhatta, D., 2014, Eq. (8.2.5)). $\text{Res}[f(x),p]$ represents the residue of function $f(x)$ at pole $x = p$.

3.3 System Model and problem formulation

Consider a wiretap system model, where a legitimate transmitter (Alice) wishes to send secret messages to an intended receiver (Bob) in the presence of a potential eavesdropper (Eve). The link between Alice and Bob is called the main channel, while the one between Alice and each Eve is named the wiretap channel. It is assumed that (i) Alice, Bob and Eve are equipped with single, M_B, and M_E antennas, respectively; (ii) the main and the wiretap channels undergo the $\alpha-\mu$ fading Yacoub (2007a), with fading parameters $\alpha_k, \mu_k, k \in \{B,E\}$; (iii) the maximum ratio combining (MRC) scheme is utilized at Bob and Eve.

For the given system configuration, the received instantaneous SNRs at Bob and Eve are receptively given as $\gamma_k = \frac{Pg_k}{\sigma_k^2} = \bar{\gamma}_k g_k$, and $g_k = \sum_{m=1}^{M_k} |h_{k,m}|^2$ represents the instantaneous channel power gain with unit mean. P, σ_B^2 and σ_E^2 denote the transmission power, noise power at Bob and Eve, respectively.

Since the probability density function (PDF) of g_k is the convolution of M_k PDFs of $h_{k,m}$, however, the high complexity of the M_k-dimensional integrals of $f_{\gamma_k}(\gamma)$ hinders the adoption of a closed-form expression for the SOP. Fortunately, as proved in (da Costa *et al.*, 2008, Eq. (28)), the PDF of γ_k can be accurately approximated to a α-μ random variable with parameters

$(\hat{\alpha}_k, \hat{\mu}_k, \hat{\Omega}_k)$[1], and is given as follows

$$f_{\gamma_k}(\gamma) \approx \frac{\hat{\alpha}_k \gamma^{\frac{\hat{\alpha}_k\hat{\mu}_k}{2}-1}}{2\hat{\Omega}_k^{\frac{\hat{\alpha}_k\hat{\mu}_k}{2}}\Gamma(\hat{\mu}_k)} \exp\left[-\left(\frac{\gamma}{\hat{\Omega}_k}\right)^{\frac{\hat{\alpha}_k}{2}}\right] \overset{(a)}{=} \kappa_k H_{0,1}^{1,0}\left[\lambda_k\gamma \middle| \begin{matrix} - \\ (\hat{\mu}_k - \frac{2}{\hat{\alpha}_k}, \frac{2}{\hat{\alpha}_k}) \end{matrix}\right], \tag{3.1}$$

where $\hat{\Omega}_k = \frac{\bar{\gamma}_k\Gamma(\hat{\mu}_k)}{\Gamma\left(\hat{\mu}_k+\frac{2}{\hat{\alpha}_k}\right)}$, $\kappa_k = \frac{1}{\hat{\Omega}_k\Gamma(\hat{\mu}_k)}$, $\lambda_k = \frac{1}{\hat{\Omega}_k}$. Step (a) is derived by using (Mathai *et al.*, 2009a, Eq. (1.125)). The cumulative distribution function (CDF) of γ_k, i.e., $F_{\gamma_k}(\gamma)$ is therefore obtained from (Bodenschatz, 1992, Eq. (3.7)) and is given by

$$F_{\gamma_k}(\gamma) = 1 - \frac{\kappa_k}{\lambda_k} H_{1,2}^{2,0}\left[\lambda_k\gamma \middle| \begin{matrix} (1,1) \\ (0,1), (\hat{\mu}_i, \frac{2}{\hat{\alpha}_i}) \end{matrix}\right] = 1 - \bar{F}_{\gamma_k}(\gamma), \tag{3.2}$$

where $\bar{F}_{\gamma_k}(\gamma)$ is the complementary CDF (CCDF).

Assuming the availability of perfect channel state information (CSI) at all terminals and the unit distance between Alice and Bob, Alice and Eve, the instantaneous secrecy capacity is given by Lei *et al.* (2017a)

$$C_s = \left[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)\right]^+. \tag{3.3}$$

3.4 Secrecy outage probability analysis

A secrecy outage event happens when either the secrecy capacity C_s is equal to 0, or when the target secrecy rate R_t is greater than the instantaneous secrecy capacity, i.e., $C_s < R_t$. Revisiting (3.3), the SOP, $\mathscr{P}_{out}$, is conceptually and mathematically defined by[2],

$$\mathscr{P}_{out} = Pr(C_s < R_t) = \int_0^\infty F_{\gamma_B}(\gamma_0) f_{\gamma_E}(\gamma_E) d\gamma_E = 1 - \int_0^\infty \bar{F}_{\gamma_B}(\gamma_0) f_{\gamma_E}(\gamma_E) d\gamma_E, \tag{3.4}$$

[1] $(\hat{\alpha}_k, \hat{\mu}_k, \hat{\Omega}_k)$ can be estimated using the moment-based approximation method proposed in (da Costa *et al.*, 2008, Eq. (22-24)).

[2] Due to the space limitation, the detailed derivation is suggested as a reference Kong *et al.* (2016a).

where $\gamma_0 = R_s\gamma_E + \mathscr{W}$, $R_s = 2^{R_t}$, $\mathscr{W} = R_s - 1$.

3.4.1 Analytical SOP

Proposition 1. *The generalized SOP expression over the SIMO $\alpha-\mu$ wiretap fading channels is given by*

$$\mathscr{P}_{out} = 1 - \frac{\kappa_B\kappa_E\mathscr{W}}{R_s\lambda_B} H_{1,0:1,1:1,1}^{0,1:0,1:1,1}\left[\frac{1}{\lambda_B\mathscr{W}}, \frac{R_s}{\lambda_E\mathscr{W}}\middle|\begin{matrix}(2,1,1)\\ -\end{matrix}\middle|\begin{matrix}(1-\hat{\mu}_B, \frac{2}{\hat{\alpha}_B})\\ (0,1)\end{matrix}\middle|\begin{matrix}(1-\hat{\mu}_E+\frac{2}{\hat{\alpha}_E}, \frac{2}{\hat{\alpha}_E})\\ (1,1)\end{matrix}\right], \tag{3.5}$$

where $H_{p,q:p_1,q_1:p_2,q_2}^{0,n:m_1.n_1:m_2,n_2}$ is the bivariate Fox's H-function.

Proof. Revisiting (3.4) and using the Parseval's relation for Mellin transform (Debnath & Bhatta, 2014, Eq. (8.3.23)), we have

$$\mathscr{I} = \int_0^\infty \bar{F}_{\gamma_B}(\gamma_0) f_{\gamma_E}(\gamma_E) d\gamma_E = \frac{1}{2\pi j}\int_{\mathscr{L}_1} \mathscr{M}[\bar{F}_{\gamma_B}(\gamma_0), 1-s]\mathscr{M}[f_{\gamma_E}(\gamma_E), s] ds, \tag{3.6}$$

where $j = \sqrt{-1}$, $\mathscr{L}_1$ is the integration path from $\upsilon - j\infty$ to $\upsilon + j\infty$, and υ is a constant Debnath & Bhatta (2014).

Then by introducing the mathematical definition of univariate Fox's H-function, and then interchanging the order of two integrals, $\mathscr{M}[\bar{F}_B(\gamma_0), 1-s]$ can be rewritten as

$$\begin{aligned}\mathscr{M}[\bar{F}_{\gamma_B}(\gamma_0), 1-s] &= \int_0^\infty \gamma_c^{-s}\bar{F}_B(\gamma_0) d\gamma_E \\ &= \frac{\kappa_B}{2\lambda_B\pi j}\int_{\mathscr{L}_2} \frac{\Gamma(\xi)\Gamma(\hat{\mu}_B + \frac{2}{\hat{\alpha}_B}\xi)}{\Gamma(1+\xi)}\lambda_B^{-\xi}\int_0^\infty \frac{{\gamma_E}^{-s}}{\gamma_0^\xi} d\gamma_E d\xi,\end{aligned} \tag{3.7}$$

where $\mathscr{L}_2$ is a certain contour separating the poles of $\Gamma(\xi)$ from the poles of $\Gamma(\hat{\mu}_B + \frac{2}{\hat{\alpha}_B}\xi)$. Next, by representing $\gamma_0 = R_s\gamma_E + \mathscr{W}$, using (Gradshteyn & Ryzhik, 2014, Eq. (3.194.3)) and the property $\mathscr{B}(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$ (Gradshteyn & Ryzhik, 2014, Eq. (8.384.1)), we obtain the

following result

$$\mathscr{M}[\bar{F}_{\gamma_B}(\gamma_0),1-s]=\frac{\kappa_B}{2\lambda_B\pi j}\left(\frac{R_s}{\mathscr{W}}\right)^{s-1}\Gamma(1-s)\int_{\mathscr{L}_2}\frac{\Gamma(\xi+s-1)\Gamma(\hat{\mu}_B+\frac{2}{\hat{\alpha}_B}\xi)}{\Gamma(1+\xi)}(\lambda_B\mathscr{W})^{-\xi}d\xi. \tag{3.8}$$

Subsequently, substituting (3.8) and the Mellin transform for $f_{\gamma_C}(\gamma_c)$ (Alhennawi, H. R., Ayadi, M. M. H. E., Ismail, M. H. & Mourad, H. A. M., 2016, eq. (5)), i.e., $\mathscr{M}[f_{\gamma_E}(\gamma_c),s]=\kappa_E\lambda_E^{-s}\Gamma(\hat{\mu}_E-\frac{2}{\hat{\alpha}_E}+\frac{s}{\hat{\alpha}_E})$ into (3.6), arrives at the following result,

$$\begin{aligned}\mathscr{I}=-\frac{\kappa_B\kappa_E\mathscr{W}}{4\lambda_B R_s\pi^2}\int_{\mathscr{L}_1}\int_{\mathscr{L}_2}&\frac{\Gamma(\xi+s-1)\Gamma(\hat{\mu}_B+\frac{2}{\hat{\alpha}_B}\xi)}{\Gamma(1+\xi)(\lambda_B\mathscr{W})^{\xi}}\\&\times\Gamma(1-s)\Gamma\left(\hat{\mu}_E-\frac{2}{\hat{\alpha}_E}+\frac{2}{\hat{\alpha}_E}s\right)\left(\frac{R_s}{\lambda_E\mathscr{W}}\right)^{s}d\xi ds,\end{aligned} \tag{3.9}$$

and subsequently applying the definition of the bivariate Fox's H-function, the proof is achieved.

□

3.4.2 Asymptotic SOP

In order to demonstrate the usefulness of the result in Proposition 1 and for the sake of highlighting the effect of channel fading parameters on the SOP, the asymptotic behavior of $\mathscr{P}_{out}$ is conducted in this subsection for different scenarios by using the residue approach given in (Chergui, H., Benjillali, M. & Saoudi, S., 2016, sec. IV). Our asymptotic results are consequently summarized in Table. 3.1.

Table 3.1 Asymptotic analysis of the $\mathscr{P}_{out}$

Scenario	**Asymptotic** $\mathscr{P}_{out}$
$\bar{\gamma}_E\to\infty$	$1-\frac{\Gamma\left(\hat{\mu}_B+\frac{\hat{\alpha}_E\hat{\mu}_E}{\hat{\alpha}_B}\right)}{\hat{\mu}_E\Gamma(\hat{\mu}_B)\Gamma(\hat{\mu}_E)}\left(\frac{\lambda_E}{R_s\lambda_B}\right)^{\frac{\hat{\alpha}_E\hat{\mu}_E}{2}}$ (3.10)
$\bar{\gamma}_B\to\infty$	$\frac{\Gamma\left(\frac{\hat{\alpha}_B\hat{\mu}_B}{\hat{\alpha}_E}+\hat{\mu}_E\right)}{\hat{\mu}_B\Gamma(\hat{\mu}_B)\Gamma(\hat{\mu}_E)}\left(\frac{R_s\lambda_B}{\lambda_E}\right)^{\frac{\hat{\alpha}_B\hat{\mu}_B}{2}}$ (3.11)

According to Chergui *et al.* (2016), expansions of the univariate and bivariate Fox's H-functions can be derived by evaluating the residue of the corresponding integrands at the closest poles to the contour, namely, the minimum pole on the right for large Fox's H-function arguments and the maximum pole on the left for small ones. In the case of $\bar{\gamma}_E \to \infty$, we have $\frac{R_s}{\lambda_E \mathscr{W}} \to \infty$. The bivariate Fox's H-function is evaluated at the highest poles on the left of $\mathscr{L}_1$, i.e., $s = 1-\xi$, therefore, it leads to the following result,

$$\begin{aligned}
&\frac{1}{2\pi j}\int_{\mathscr{L}_1} \underbrace{\Gamma(\xi+s-1)\Gamma(1-s)\Gamma\left(\hat{\mu}_E - \frac{2}{\hat{\alpha}_E} + \frac{2}{\hat{\alpha}_E}s\right)\left(\frac{R_s}{\lambda_E \mathscr{W}}\right)^s}_{\psi(s)} ds \\
&\approx \mathrm{Res}[\psi(s), 1-\xi] = \lim_{s\to 1-\xi}(s+\xi-1)\psi(s) \\
&= \Gamma(\xi)\Gamma\left(\hat{\mu}_E - \frac{2}{\hat{\alpha}_E}\xi\right)\left(\frac{R_s}{\lambda_E \mathscr{W}}\right)^{1-\xi}.
\end{aligned} \tag{3.12}$$

Therefore, we have

$$\begin{aligned}
\mathscr{P}_{out} &\approx 1 - \frac{\kappa_B \kappa_E}{2\lambda_B \lambda_E \pi j}\int_{\mathscr{L}_2} \underbrace{\frac{\Gamma(\xi)\Gamma\left(\hat{\mu}_E - \frac{2}{\hat{\alpha}_E}\xi\right)\Gamma\left(\hat{\mu}_B + \frac{2}{\hat{\alpha}_B}\xi\right)}{\Gamma(1+\xi)\left(\frac{\lambda_B R_s}{\lambda_E}\right)^{\xi}}}_{\tau(\xi)} d\xi \\
&= 1 - \frac{1}{\Gamma(\hat{\mu}_B)\Gamma(\hat{\mu}_E)} H_{2,2}^{2,1}\left[\frac{\lambda_B R_s}{\lambda_E}\middle|\begin{matrix}(1-\hat{\mu}_E, \frac{2}{\hat{\alpha}_E}),(1,1)\\ (0,1),(\hat{\mu}_B, \frac{2}{\hat{\alpha}_B})\end{matrix}\right].
\end{aligned} \tag{3.13}$$

In continuation, (3.13) can be successively and asymptotically simplified as (10) by computing the highest pole on the right of the contour $\mathscr{L}_2$, namely $\xi = \frac{\hat{\alpha}_E \hat{\mu}_E}{2}$,

$$\mathscr{P}_{out} \approx 1 - \frac{\kappa_B \kappa_E}{\lambda_B \lambda_E}\mathrm{Res}\left[\tau(\xi), \frac{\hat{\alpha}_E \hat{\mu}_E}{2}\right], \tag{3.14}$$

and then applying $\frac{\kappa_k}{\lambda_k} = \frac{1}{\Gamma(\hat{\mu}_k)}$, the proof for (10) is achieved.

Following the same methodology, the proof for the case, $\bar{\gamma}_B \to \infty$, can be similarly achieved by first computing (3.9) at the highest pole of $\mathscr{L}_2$ at $\xi = 1 - s$, and subsequently evaluating the obtained result at the poles of $\mathscr{L}_1$, i.e., $s = 0$ and $s = \frac{\hat{\alpha}_B \hat{\mu}_B}{2}$, respectively.

Remark 1. From the definition of SOP,

$$\mathscr{P}_{out} = \mathscr{P}r(\gamma_B \leq R_s\gamma_E + \mathscr{W}) \geq \underbrace{\mathscr{P}r(\gamma_B \leq R_s\gamma_E)}_{\mathscr{P}^L_{out}} = \int_0^\infty F_{\gamma_B}(R_s\gamma_E) f_{\gamma_E}(\gamma_E) d\gamma_E, \tag{3.15}$$

then plugging (3.1) and (3.2) into (3.15), using the Mellin transform of the products of two Fox's H-functions (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), $\mathscr{P}^L_{out}$ is finally given by (3.13).

Remark 2. Conclusively speaking, the results shown by (10), (11) and (3.13) do not vary with $\theta = \frac{\bar{\gamma}_B}{\bar{\gamma}_E}$.

Remark 3. The secrecy diversity order at Bob is defined as $D_{sec} \triangleq -\lim_{\bar{\gamma}_B \to \infty} \frac{\log(\mathscr{P}^\infty_{out})}{\log(\bar{\gamma}_B)}$ Liu, Y., Qin, Z., Elkashlan, M., Gao, Y. & Hanzo, L. (2017), and $\mathscr{P}^\infty_{out}$ is given by (11). After some algebraic manipulations, the diversity order is finally given by, $D_{sec} = \frac{\hat{\alpha}_B \hat{\mu}_B}{2}$.

3.5 Numerical results and discussions

In this section, we confirm the accuracy of our analytical derivations demonstrated in Section 3.4, in comparison with the Monte-Carlo (MC) simulation results[3]. It is noted that the bivariate Fox's H-function can be easily and efficiently implemented at MATLAB (Peppas, K. P., Lazarakis, F., Alexandridis, A. & Dangakis, K., 2012, Table. II), Python Alhennawi *et al.* (2016) and Mathematica Lei *et al.* (2015)[4].

Fig. 3.1(a) verifies the derived SOP and $\mathscr{P}^L_{out}$ against $\bar{\gamma}_B$ over SISO[5] $\alpha - \mu$ wiretap channels. As seen from the figure, our derivation perfectly matches with the simulation outcomes, even

[3] The $\alpha - \mu$ fading channel is implemented by using the WAFO toolboxBrodtkorb *et al.* (2000).

[4] It is worthy to mention that the numerical evaluation of the bivariate and univariate Fox's H-function for MATLAB implementations is based on the method proposed in (Peppas, K. P., 2012, Appendix. A) and (Peppas *et al.*, 2012, Table. II), respectively.

[5] It is noted when $M_B = M_E = 1$, the SIMO $\alpha - \mu$ fading channel is reduced to the SISO $\alpha - \mu$ fading channels, henceforth, we have $\alpha_B = \hat{\alpha}_B$, and $\alpha_E = \hat{\alpha}_E$.

for several specific combinations of different values for α and μ, which correspond to Rayleigh ($\alpha = 2,\ \mu = 1$), Nakagami-m ($\alpha = 2,\ \mu = m$) and Weibull (α is the fading parameter, and $\mu = 1$) fading channels, respectively. In addition, our derived $\mathscr{P}_{out}^{L}$ keeps consistent with the result given in (Lei *et al.*, 2015, eq.(11))[6]. Figs. 3.1 (b) and 3.2 plot the asymptotic SOP against $\bar{\gamma}_B$ and $\bar{\gamma}_E$, respectively, it can be seen that the results given in (10) and (11) are becoming tight at high SNR regime.

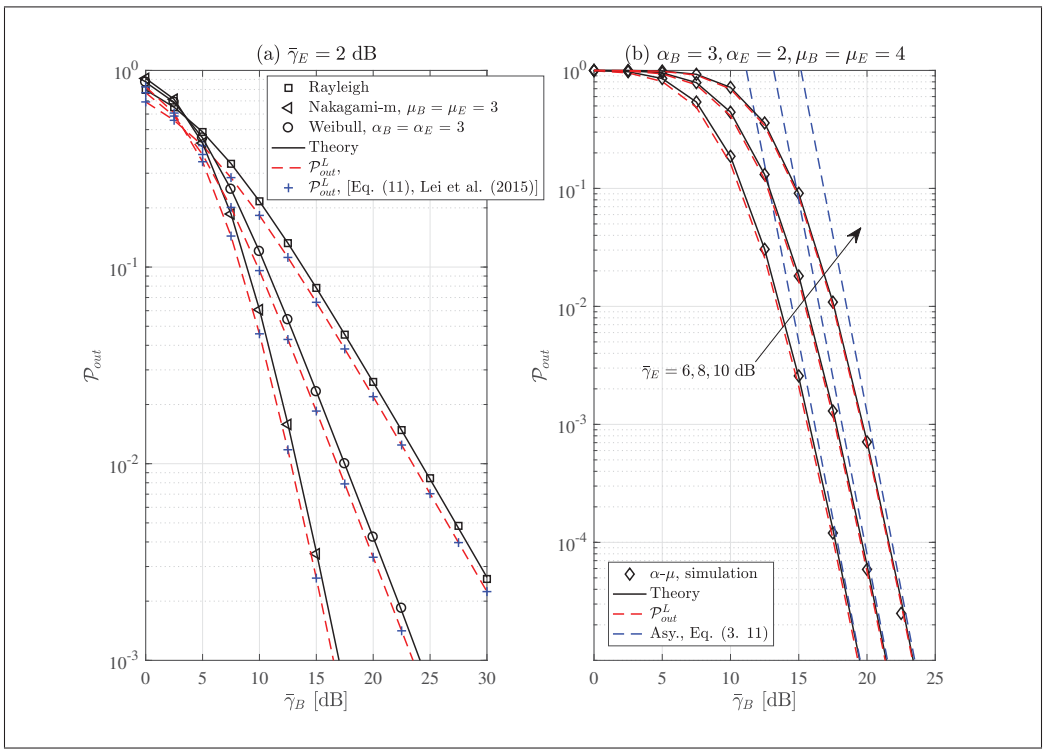


Figure 3.1 $\mathscr{P}_{out}$ versus $\bar{\gamma}_B$ when $R_t = 0.5$ and $M_B = M_E = 1$

In Fig. 3.3, the comparison of the analytical expressions for the $\mathscr{P}_{out}$, with simulation results regarding different (M_B, M_E), are performed. As suggested in the figure, the $\mathscr{P}_{out}$ is, as expected, increased with the increase of M_E, and decreased with the increase of M_B.

[6] The MC simulation in Lei *et al.* (2015) is used to confirm the lower bound of SOP, whereas the MC simulation herein is supposed to confirm the exact SOP.

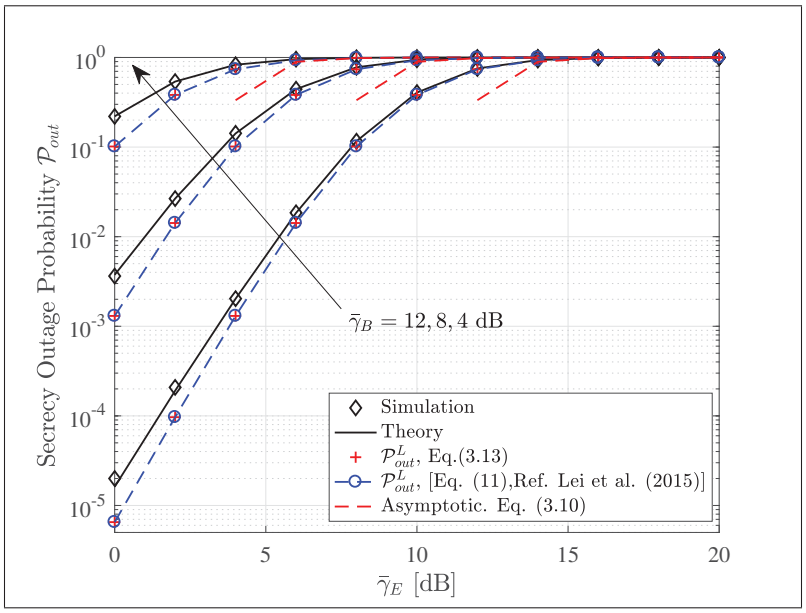


Figure 3.2 $\mathscr{P}_{out}$ versus $\bar{\gamma}_E$ when $R_t = 0.5$, $\alpha_B = 3, \alpha_E = 2, \mu_B = \mu_E = 4$, and $M_B = M_E = 1$

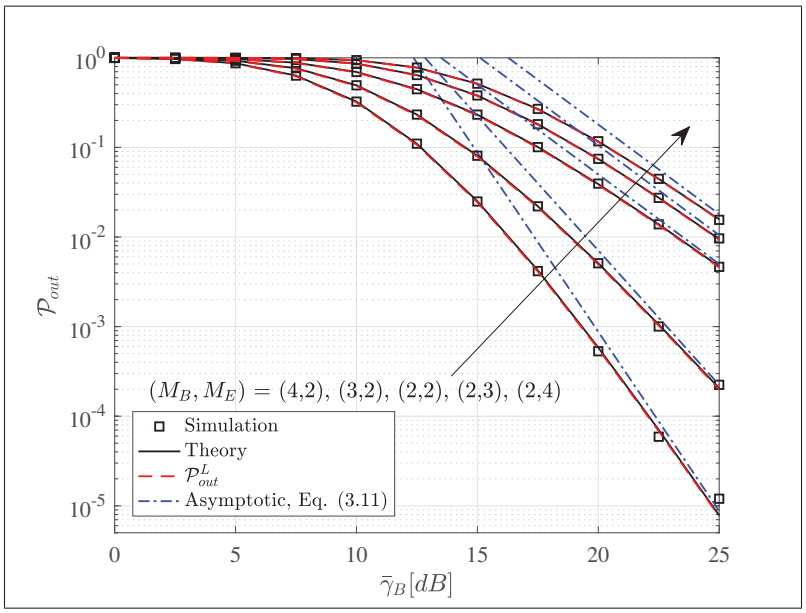


Figure 3.3 $\mathscr{P}_{out}$ versus $\bar{\gamma}_B$ for selected values of M_B, M_E when $R_t = 0.5$, $\bar{\gamma}_E$ = 10 dB, $\alpha_B = \alpha_E$ = 2, $\mu_B = 1$, $\mu_E = 2$

As observed in Figs. 3.1 and 3.3, one can grasp the following outcome about the asymptotic behavior of $\mathscr{P}_{out}$: (i) the lower bound of SOP given by (3.13) is becoming tight and closely approximates the analytical $\mathscr{P}_{out}$, as $\bar{\gamma}_E$ increases; (ii) our derived asymptotic SOP given by (11) is gradually approaching the analytical results, especially at high SNR $\bar{\gamma}_E$ regime. As discussed in Remark. 2 and plotted in Fig. 3.4, the $\mathscr{P}^L_{out}$ and the asymptotic SOP at high SNR regime are only varying with the change of θ.

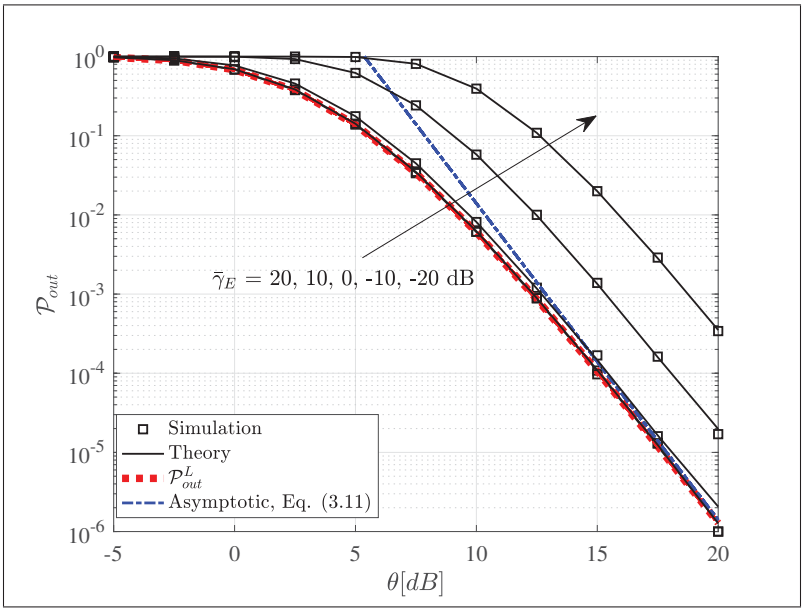


Figure 3.4 $\mathscr{P}_{out}$ versus θ when $R_t = 0.5$, $M_B = M_E = 2$, $\alpha_B = \alpha_E = 2$, $\mu_B = \mu_E = 2$, and $\bar{\gamma}_B = \theta\bar{\gamma}_E$

3.6 Conclusions

In this letter, we presented the novel, highly accurate and asymptotic closed-form expressions for the SOP over the SIMO $\alpha - \mu$ wiretap channels. The Monte-Carlo simulation was performed and compared with our mathematical representations. Useful insights can be summarized as (i) the highly accurate expression seems cumbersome, but it is in perfect agreement with numerical results; (ii) the lower bound of SOP closely approximates the analytical SOP especially at high $\bar{\gamma}_E$ regime; (iii) the obtained result is extremely general and advantageous

when the main channel and wiretap channel undergo different small-scale fading effects; (iv) on the other hand, the MIMO $\alpha - \mu$ wiretap fading channel presents a particular challenge as beamforming is generally required whereas for SISO and SIMO scenarios, only codebook generation and power allocation are involved. The authors believe that MIMO systems require a special treatment, hence this scenario is left for future work.

CHAPTER 4

ON PHYSICAL LAYER SECURITY OVER THE FISHER-SNEDECOR $\mathscr{F}$ WIRETAP FADING CHANNELS

Long Kong and Georges Kaddoum

Département de Génie électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3.

Paper published in *IEEE ACCESS*, December 2018.

4.1 Abstract

In this paper, we initially investigate the physical layer security over device-to-device (D2D) communications, where the channel is modeled from the Fisher-Snedecor $\mathscr{F}$ distribution. To be specific, secrecy metrics, including the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), and the average secrecy capacity (ASC), are well derived with exact closed-form expressions, which are given in terms of the Meijer's *G*-function. The accuracies of our mathematical expressions are further validated by Monte-Carlo simulation results.

Keywords: Physical layer security, Fisher-Snedecor $\mathscr{F}$ wiretap fading channels, Meijer's *G*-function.

4.2 Introduction

Currently, D2D communication is widely regarded as a promising candidate for the fifth-generation (5G) communication. Due to the highly standardization of the communication scheme, including the modulation and coding mechanism Zou, Y., Zhu, J., Wang, X. & Leung, V. C. M. (2015), it is increasingly vulnerable for legitimate D2D pairs to highly ensure secrecy from malicious third entities, especially when they are being wiretapped due to the open access of transmission medium Shiu *et al.* (2011).

More recently, the Fisher-Snedecor $\mathscr{F}$ fading model was proposed in Yoo, S. K., Cotton, S. L., Sofotasios, P. C., Matthaiou, M., Valkama, M. & Karagiannidis, G. K. (2017) to characterize the D2D links. It is reported therein that the Fisher-Snedecor $\mathscr{F}$ distribution can provide a good, and in most cases, a better fit to the experimental channel data, especially in comparison with another composite fading model, i.e., the generalized-K distribution. The seminal finding in Yoo *et al.* (2017) demonstrates that the Fisher-Snedecor $\mathscr{F}$ fading model is a promising alternative model to capitalize the device-to-device (D2D) communication links, especially at 5.8 GHz, for both indoor and outdoor environments Rahama, Y. A., Ismail, M. H. & Hassan, M. (2018).

In addition, the probability density function (PDF) of Fisher-Snedecor $\mathscr{F}$ distribution is less simpler than the generalized-K distribution due to the PDF of generalized-K distribution having the non-elementary function, i.e., the modified Bessel function. In addition, the Fisher-Snedecor $\mathscr{F}$ distribution is flexible since it can be reduced to some special cases when the fading parameters are fixed for some values Badarneh, O. S., da Costa, D. B., Sofotasios, P. C., Muhaidat, S. & Cotton, S. L. (2018), i.e., Nakagami-m distribution ($m_{s,l} \to \infty, m_l = m$), Rayleigh distribution ($m_{s,l} \to \infty, m_l = 1$), and one-sided Gaussian distribution ($m_{s,l} \to \infty, m_l = 0.5$).

As it can be seen from the existing works Lei, H., Ansari, I. S., Gao, C., Guo, Y., Pan, G. & Qaraqe, K. A. (2016a); Lei, H., Gao, C., Ansari, I. S., Guo, Y., Pan, G. & Qaraqe, K. A. (2016b); Lei, H., Zhang, H., Ansari, I. S., Gao, C., Guo, Y., Pan, G. & Qaraqe, K. A. (2016c); Wu, L., Yang, L., Chen, J. & Alouini, M. S. (2018a), the secrecy concern over the generalized-K wiretap fading models has been widely investigated. In Lei *et al.* (2016b), the lower bound of secrecy outage probability and average secrecy capacity over the single-input and multiple-output (SIMO) generalized-K wiretap fading model were derived, which were given in terms of the Meijer's G-function. This function is with a general form and is defined in terms of the Mellin-Barnes integral. In addition, it has been found widely applied in literature Kong *et al.* (2018a); Kong, L., Kaddoum, G. & Vuppala, S. (2018d); Lei *et al.* (2015,1,1,1,1); Moualeu, J. M. & Hamouda, W. (2017); Wu *et al.* (2018a) when analyzing secrecy performance over

various fading channels, for example, $\alpha-\mu$ Kong *et al.* (2016b,1,1); Lei *et al.* (2015,1) and $\kappa-\mu$ Moualeu & Hamouda (2017), etc.

Motivated by the experimental and theoretical advantages of Fisher-Snedecor $\mathscr{F}$ distribution, as such, the objectives of this paper are multi-fold,

- Considering the presence of an active eavesdropper, two essential secrecy metrics, including the secrecy outage probability (SOP) and the probability of non-zero secrecy capacity (PNZ), are derived with exact closed-form expressions, moreover, the lower bound of SOP is also provided. The aforesaid metrics are exactly given either in terms of the univariate Meijer's *G*-function or the bivariate Meijer's *G*-function.

- On the other hand, considering a passive eavesdropper, this paper is subjective to analyze the average secrecy capacity (ASC) of a D2D network over the Fisher-Snedecor $\mathscr{F}$ wiretap fading channels. Hence, the ASC is mathematically derived in terms of the univariate and bivariate Merjer's *G*-functions. Even though the Meijer's *G*-function is a non-elementary function, the implementation of univariate Meijer's *G*-function is already available in mathematical software packages, like Matlab2017b, Mathematica Mei and Maple. In order to gain more insights at high signal-to-noise ratio (SNR) regime, the bivariate Merjer's *G*-function is further simplified in terms of the univariate Merjer's *G*-function. In addition, the correctness of our analytical results are verified by Monte-Carlo simulation results.

Finally, the practical benefit of having such analytical secrecy expressions allows wireless system designers to have a quick system evaluation when facing security risks.

The rest of this paper is outlined as follows: Section 4.3 presents the system model. Sections 4.4, 4.5, and 4.6 provide the secrecy analysis. Numerical results and discussion are subsequently presented in Section 4.7, followed with concluding remarks in Section 4.8.

Mathematical Functions and Notations: $\Gamma(.)$ is the complete Gamma function (Gradshteyn & Ryzhik, 2014, eq. (8.310.1)). $\mathscr{B}(x,y)$ is the Beta function. ${}_2F_1(a,b;c;x)$ is the Gauss hypergeometric function. $G_{p,q}^{m,n}[.]$ is the univariate Meijer's *G*-function (Gradshteyn & Ryzhik, 2014, eq.

(9.301)), $G_{p,q:p_1,q_1:p_2,q_2}^{m,n:m_1,n_1:m_2,n_2}[.]$ is the bivariate Meijer's G-function. $\mathscr{B}(x,y)$ is the Beta function (Gradshteyn & Ryzhik, 2014, eq. (8.380.1)). ${}_2F_1(a,b;c;x)$ is the Gauss hypergeometric function (Gradshteyn & Ryzhik, 2014, eq.(9.14.2)). $\mathscr{M}[f(x),s]$ denotes the Mellin transform of $f(x)$ (Debnath & Bhatta, 2014, eq. (8.2.5)). $\text{Res}[f(x),p]$ represents the residue of function $f(x)$ at pole $x=p$.

4.3 System Model

Consider the Wyner's wiretap channel model Wyner (1975), to be specific, as shown in Fig. 4.1, a wireless D2D link in the presence of an eavesdroppers, where the source (Alice) intends to send private messages to legitimate receiver (Bob) over the main channel h_B, and being intercepted by a third entity (Eve) over the wiretap channel h_E.

It is assumed that (i) all users are single antenna based; (ii) the D2D links are modeled by the independent Fisher-Snedecor $\mathscr{F}$ distribution Yoo *et al.* (2017), $h_k, k \in \{B,E\}$ with fading parameters $(m_{k,s}, m_k)$, herein $m_{k,s}, m_k$ represent the amount of shadowing of the root-mean-square (rms) signal power and the fading severity parameter, respectively.

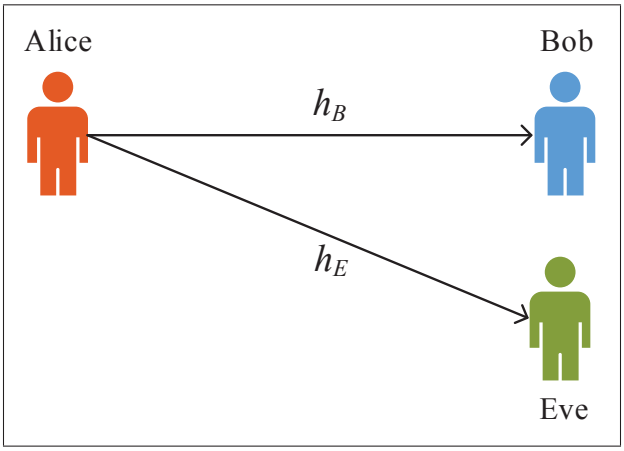


Figure 4.1 Illustration of system model with two legitimate transceivers (Alice and Bob) and one eavesdropper (Eve)

For the given system configuration, the received instantaneous signal-to-noise ratios (SNRs) at Bob and Eve are expressed as

$$\gamma_k = \frac{P g_k}{\sigma_k^2} = \bar{\gamma}_k g_k \tag{4.1}$$

where P, σ_B^2, and σ_E^2 denote the transmission power, noise power at Bob and Eve, respectively. $g_k = |h_k|^2$ represents the instantaneous channel power gain with unit mean. It is assumed that both the main channel (Alice $\rightarrow$ Bob) and the wiretap channel (Alice $\rightarrow$ Eve) are quasi-static fading channels Bloch *et al.* (2008).

The PDF of the instantaneous received SNR, γ_k, is defined in (Yoo *et al.*, 2017, eq. (5)), we further rewrite it in terms of the Meijer's G-function from (Prudnikov *et al.*, 1990, eq. (8.4.2.5)) and (Gradshteyn & Ryzhik, 2014, eq.(9.31.5)),

$$f_k(\gamma) = \frac{m_k^{m_k} (m_{k,s}\bar{\gamma}_k)^{m_{k,s}} \gamma^{m_k - 1}}{\mathscr{B}(m_k, m_{k,s})(m_k\gamma + m_{k,s}\bar{\gamma}_k)^{m_k + m_{k,s}}} \tag{4.2}$$

$$= \mathscr{C}_k G_{1,1}^{1,1}\left[\lambda_k \gamma \middle| \begin{matrix} -m_{k,s} \\ m_k - 1 \end{matrix} \right], \tag{4.3}$$

where $\lambda_k = \frac{m_k}{m_{k,s}\bar{\gamma}_k}$ and $\mathscr{C}_k = \frac{\lambda_k}{\Gamma(m_k)\Gamma(m_{k,s})}$.

The cumulative distribution function (CDF) of γ_k, i.e., $F_k(\gamma)$ is defined in (Yoo *et al.*, 2017, eq. (11)) and given by

$$F_k(\gamma) = \frac{\gamma^{m_k} {}_2F_1\left(m_k + m_{k,s}, m_k; m_k + 1; -\frac{m_k\gamma}{m_{k,s}\bar{\gamma}_k}\right)}{m_k^{1-m_k}\mathscr{B}(m_k, m_{k,s})(m_{k,s}\bar{\gamma}_k)^{m_k}} \tag{4.4}$$

$$\overset{(a)}{=} \Phi_k G_{2,2}^{1,2}\left[\lambda_k \gamma \middle| \begin{matrix} (1 - m_{k,s}, 1) \\ (m_k, 0) \end{matrix} \right], \tag{4.5}$$

where $\Phi_k = \frac{\Gamma(m_k+1)}{m_k\Gamma(m_k)\Gamma(m_k+m_{k,s})\mathscr{B}(m_k,m_{k,s})}$, and step (a) is similarly developed from (Prudnikov *et al.*, 1990, eq. (8.4.49.13)).

Assuming the availability of perfect channel state information (CSI) at all terminals, the instantaneous secrecy capacity is defined as the difference between the main channel capacity C_M and the wiretap channel capacity C_W Lei *et al.* (2016c), and is expressed as follows

$$C_s(\gamma_B,\gamma_E)=\begin{cases}C_M-C_W, & \gamma_B>\gamma_E\\ 0, & \text{otherwise}\end{cases}=\begin{cases}\log_2\left(\frac{1+\gamma_B}{1+\gamma_E}\right), & \gamma_B>\gamma_E\\ 0, & \text{otherwise.}\end{cases} \tag{4.6}$$

4.4 SOP Characterization

When considering an active eavesdropper, secrecy outage probability (SOP) is frequently measured as a benchmark to indicate how secure the Alice-Bob transceiver pair is.

The SOP is an information-theoretical concept having a definition that a secrecy outage event happens when the instantaneous secrecy capacity C_s is equal to 0, or when C_s is lower than the target secrecy rate, i.e., $C_s < R_t$.

To this end, making a revisit to (4.6), the secrecy outage probability, $\mathscr{P}_{out}(R_t)$, is conceptually and mathematically explained in the following form Kong *et al.* (2016a,1).

$$\mathscr{P}_{out}(R_t)=\mathscr{P}r(C_s<R_t)=\mathscr{P}r(\gamma_B\leq R_s\gamma_E+R_s-1)=\int_0^{\infty}F_B(\gamma_0)f_E(\gamma_E)d\gamma_E, \tag{4.7}$$

where $\gamma_0=R_s\gamma_E+R_s-1=R_s\gamma+\mathscr{W}$, $R_s=2^{R_t}$, $\mathscr{W}=R_s-1$.

Proposition 2. The secrecy outage probability over Fisher-Snedecor $\mathscr{F}$ Wiretap Fading Channels is given either in terms of the extended generalized bivariate Merjer's *G*-function, shown in (4.8a),

$$\mathscr{P}_{out,1}=\frac{\Phi_B\mathscr{C}_E\mathscr{W}}{R_s}G^{0,1:2,1:1,1}_{1,0:2,3:1,1}\left[\frac{R_s}{\lambda_E\mathscr{W}},\frac{1}{\lambda_B\mathscr{W}}\middle|\begin{matrix}(2,1,1)\\ -\end{matrix}\middle|\begin{matrix}(1-m_B,1)\\ (0,m_{B,s},1)\end{matrix}\middle|\begin{matrix}(2-m_E)\\ (1,1+m_{E,s})\end{matrix}\right], \tag{4.8a}$$

or the univariate Merjer's G-function shown in (4.8b),

$$\mathscr{P}_{out,2} = \frac{\Phi_B \mathscr{C}_E}{\lambda_B R_s} \sum_{n=1}^{\infty} \frac{(-\lambda_B \mathscr{W})^n}{n!} G_{4,4}^{3,3} \left[\frac{\lambda_E}{\lambda_B R_s} \middle| \begin{matrix} (0, -m_{E,s}, n-m_B, n) \\ (m_E-1, n-1+m_{B,s}, n-1, n) \end{matrix} \right], \tag{4.8b}$$

where $G_{p,q:p_1,q_1:p_2,q_2}^{m,n:m_1.n_1:m_2,n_2}[.]$ is the bivariate Meijer's G-function, $G_{p,q}^{m,n}[.]$ is the univariate Meijer's G-function.

Proof. See Appendix. I.1 and Appendix. I.2 for the proofs of (4.8a) and (4.8b), respectively. □

Remark 4. *The $\mathscr{P}_{out}$ is lower bounded by*

$$\mathscr{P}_{out}^{L} = \frac{\Phi_B \mathscr{C}_E}{\lambda_E} G_{3,3}^{2,3} \left[\frac{\lambda_B R_s}{\lambda_E} \middle| \begin{matrix} (1-m_{B,s}, 1, 1-m_E) \\ (0, m_{E,s}, m_B) \end{matrix} \right]. \tag{4.9}$$

Proof. Revisiting (4.7), we have

$$\mathscr{P}_{out} = \mathscr{P}r(\gamma_B \leq R_s \gamma_E + \mathscr{W}) \geq \underbrace{\mathscr{P}r(\gamma_B \leq R_s \gamma_E)}_{\mathscr{P}_{out}^{L}} = \int_0^{\infty} F_B(R_s \gamma_E) f_E(\gamma_E) d\gamma_E. \tag{4.10}$$

Substituting (4.3) and (4.5) into (4.10), and then applying Mellin transform of the product of two Meijer's G-functions from (Prudnikov *et al.*, 1990, eqs.(2.25.1.1) and (8.3.2.21)), the proof is achieved. □

4.5 PNZ Characterization

The existence of non-zero secrecy capacity is a fundamental metric, and it is assured with the probability given by

$$\mathscr{P}_{nz} = \mathscr{P}r(\gamma_B > \gamma_E) = \int_0^{\infty} F_E(\gamma_B) f_B(\gamma_B) d\gamma_B. \tag{4.11}$$

Proposition 3. *The probability of non-zero secrecy capacity over Fisher-Snedecor $\mathscr{F}$ Wiretap Fading Channels is given by*

$$\mathscr{P}_{nz} = \frac{\mathscr{C}_B \Phi_E}{\lambda_B} G_{3,3}^{2,3}\left[\frac{\lambda_E}{\lambda_B}\middle| \begin{matrix}(1-m_{E,s}, 1-m_B, 1)\\ (0, m_{B,s}, m_E)\end{matrix}\right]. \tag{4.12}$$

Proof. Following the proof of **remark**. 4, the proof of $\mathscr{P}_{nz}$ is similarly obtained. □

4.6 ASC Characterization

4.6.1 Exact ASC

Theorem 1. *The average secrecy capacity over Fihser-Snedecor $\mathscr{F}$ wiretap fading channels is given by*

$$\begin{aligned}\bar{C}_s = &\underbrace{\frac{\mathscr{C}_B \Phi_E}{\lambda_B \ln(2)} G_{1,1:2,2:2,2}^{1,1:1,2:1,2}\left[\frac{\lambda_E}{\lambda_B}, \frac{1}{\lambda_B}\middle| \begin{matrix}(m_B)\\ (m_{B,s})\end{matrix}\middle| \begin{matrix}(1-m_{E,s}, 1)\\ (m_E, 0)\end{matrix}\middle| \begin{matrix}(1,1)\\ (1,0)\end{matrix}\right]}_{\mathscr{I}_1}\\ &+\underbrace{\frac{\mathscr{C}_E \Phi_B}{\lambda_E \ln(2)} G_{1,1:2,2:2,2}^{1,1:1,2:1,2}\left[\frac{\lambda_B}{\lambda_E}, \frac{1}{\lambda_E}\middle| \begin{matrix}(m_E)\\ (m_{E,s})\end{matrix}\middle| \begin{matrix}(1-m_{B,s}, 1)\\ (m_B, 0)\end{matrix}\middle| \begin{matrix}(1,1)\\ (1,0)\end{matrix}\right]}_{\mathscr{I}_2}\\ &-\underbrace{\frac{\mathscr{C}_E}{\lambda_E \ln 2} G_{3,3}^{2,3}\left[\frac{1}{\lambda_E}\middle| \begin{matrix}(1,1,1-m_E)\\ (1, m_{E,s}, 0)\end{matrix}\right]}_{\mathscr{I}_3}.\end{aligned} \tag{4.13}$$

Proof. Recalling the result given in (Lei *et al.*, 2016b, eq.(17)), the ASC given in (4.6) can be further mathematically expressed as

$$\bar{C}_s = \int_0^\infty \int_0^\infty C_s(\gamma_B, \gamma_E) f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_B d\gamma_E = \mathscr{I}_1 + \mathscr{I}_2 - \mathscr{I}_3, \tag{4.14}$$

where

$$\mathscr{I}_1 = \int_0^\infty \log_2(1+\gamma_B) f_B(\gamma_B) F_E(\gamma_B) d\gamma_B, \tag{4.15a}$$

$$\mathscr{I}_2 = \int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) F_B(\gamma_E) d\gamma_E, \tag{4.15b}$$

$$\mathscr{I}_3 = \int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) d\gamma_E. \tag{4.15c}$$

Next, re-expressing the logarithm function in terms of the Meijer's *G*-function Prudnikov *et al.* (1990), i.e.,

$$\log_2(1+x) = \frac{1}{\ln(2)} G_{2,2}^{1,2}\left[x \middle| \begin{matrix} (1,1) \\ (1,0) \end{matrix} \right], \tag{4.16}$$

substituting (4.3), (4.5), and (4.16) into (4.15a), $\mathscr{I}_1$ can be developed in (4.17),

$$\begin{aligned} \mathscr{I}_1 &= \frac{\mathscr{C}_B \Phi_E}{\ln(2)} \int_0^\infty G_{2,2}^{1,2}\left[\gamma \middle| \begin{matrix} (1,1) \\ (1,0) \end{matrix} \right] G_{1,1}^{1,1}\left[\lambda_B \gamma \middle| \begin{matrix} -m_{B,s} \\ m_B - 1 \end{matrix} \right] G_{2,2}^{1,2}\left[\lambda_E \gamma \middle| \begin{matrix} (1-m_{E,s},1) \\ (m_E,0) \end{matrix} \right] d\gamma \\ &= \frac{\mathscr{C}_B \Phi_E}{\ln(2)} \int_{\mathscr{L}_1} \frac{\Gamma(m_E+s)\Gamma(m_{E,s}-s)\Gamma(-s)}{\Gamma(1-s)\lambda_E^s} \underbrace{\int_0^\infty \gamma^{-s} G_{2,2}^{1,2}\left[\gamma \middle| \begin{matrix} (1,1) \\ (1,0) \end{matrix} \right] G_{1,1}^{1,1}\left[\lambda_B \gamma \middle| \begin{matrix} -m_{B,s} \\ m_B - 1 \end{matrix} \right] d\gamma}_{U} ds, \end{aligned} \tag{4.17}$$

where $\mathscr{L}_1$ is a certain contour separating the poles of $\Gamma(m_E+s)$ from the poles of $\Gamma(-s)$.

The inner integral U can be directly developed by using the Mellin transform for the product of two Meijer's *G*-functions (Prudnikov *et al.*, 1990, eq. (2.25.1.1)) as follows

$$U = \lambda_B^{s-1} G_{3,3}^{2,3}\left[\frac{1}{\lambda_B} \middle| \begin{matrix} (1,1,s-1-m_B) \\ (1,m_{B,s}+s,0) \end{matrix} \right], \tag{4.18}$$

subsequently, rewriting (4.18) in terms of the definition of univariate Meijer's *G*-function, then substituting the obtained result into (4.17) and performing the change of variables $s = -s$ and

$\xi = -\xi$, leads to the following result

$$\begin{aligned}\mathscr{I}_1 = &-\frac{\mathscr{C}_B\Phi_E}{4\ln(2)\lambda_B\pi^2}\int_{\mathscr{L}_1}\int_{\mathscr{L}_2}\frac{\Gamma(m_{B,s}-s-\xi)\Gamma(s)}{\Gamma(1+s)\Gamma(1+\xi)}\Gamma(m_B+s+\xi)\Gamma(m_E-s)\Gamma(m_{E,s}+s)\\ &\times\Gamma^2(\xi)\Gamma(1-\xi)\left(\frac{1}{\lambda_B}\right)^{\xi}\left(\frac{\lambda_E}{\lambda_B}\right)^{s}d\xi ds,\end{aligned} \tag{4.19}$$

where $\mathscr{L}_2$ is another contour, next, recognizing the definition of bivariate Meijer's G-function Gupta, S. (1969), the proof of $\mathscr{I}_1$ is accomplished.

Similarly, following the same methodology, the proof for $\mathscr{I}_2$ is achieved. With the help of (Prudnikov *et al.*, 1990, eqs. (2.25.1.1) and (8.3.2.21)), the proof of $\mathscr{I}_3$ is obtained. □

4.6.2 Asymptotic ASC

Observed from (4.13), the exact ASC is given in terms of the extended generalized bivariate Meijer's G-function. Its implementation is not available in mathematical packages, like Mathematica, Maple or MATLAB. Fortunately, it is computationally tractable and programmable, which can be found available in Peppas (2012). As such, the asymptotic ASC is derived especially when $\beta = \frac{\bar{\gamma}_B}{\bar{\gamma}_E}$ is at high SNR regime.

Theorem 2. *When $\beta = \frac{\bar{\gamma}_B}{\bar{\gamma}_E}$ is at high SNR region, the asymptotic ASC would be given by*

$$\bar{C}_s \approx \hat{I}_1 + \hat{I}_2 - \mathscr{I}_3, \tag{4.20}$$

where $\hat{I}_1$ and $\hat{I}_2$ are respectively given by (4.21a) and (4.21b),

$$\begin{aligned}\hat{I}_1 \approx &\frac{\mathscr{C}_B\Phi_E\Gamma(m_{B,s}+m_B)}{\ln(2)\lambda_B}\left(\frac{\lambda_B}{\lambda_E}\right)^{m_B}G_{4,4}^{3,3}\left[\lambda_E\left|\begin{matrix}(0,1+m_B,1-m_{E,s}+m_B,1)\\(0,0,m_B+m_E,m_B)\end{matrix}\right.\right]\\ &+\frac{\mathscr{C}_B\Phi_E\Gamma(m_E)\Gamma(m_{E,s})}{\ln(2)\lambda_B}G_{3,3}^{3,2}\left[\lambda_B\left|\begin{matrix}(0,1-m_{B,s},1)\\(0,0,m_B)\end{matrix}\right.\right],\end{aligned} \tag{4.21a}$$

$$\begin{aligned}\hat{I}_2 \approx & \frac{\mathscr{C}_E \Phi_B \Gamma(m_E + m_{E,s})}{\ln(2)\lambda_E} \left(\frac{\lambda_B}{\lambda_E}\right)^{m_{E,s}} G_{4,4}^{3,3}\left[\lambda_B \middle| \begin{matrix}(1, 1+m_{E,s}, 1-m_{E,s}-m_{B,s}, 1)\\ (0, 0, m_B - m_E, -m_{E,s})\end{matrix}\right] \\ & + \frac{\mathscr{C}_E \Phi_B \Gamma(m_B)\Gamma(m_B + m_{B,s})}{\ln(2)\lambda_E \Gamma(1+m_B)} \left(\frac{\lambda_B}{\lambda_E}\right)^{m_B} G_{3,3}^{3,2}\left[\lambda_E \middle| \begin{matrix}(1, 1-m_{E,s}+m_B, 1)\\ (0, 0, m_B + m_E)\end{matrix}\right].\end{aligned} \tag{4.21b}$$

Proof. Recalling the residue approach given in (Chergui *et al.*, 2016, Sec. IV) and the expansion principle for Meijer's *G*-function (Karagiannidis, G. K., Sagias, N. C. & Mathiopoulos, P. T., 2007, Appendix), when $\beta \to \infty$, $\frac{\lambda_E}{\lambda_B} \to \infty$, making the change of variable $s = -s$, we have

$$\mathscr{G}_1 = \frac{1}{2\pi j}\int_{\mathscr{L}_1} \underbrace{\frac{\Gamma(m_{B,s}+s-\xi)\Gamma(m_B - s + \xi)}{\Gamma(1-s)}\Gamma(m_E+s)\Gamma(m_{E,s}-s)\Gamma(-s)\left(\frac{\lambda_B}{\lambda_E}\right)^s}_{J_1(s)} ds, \tag{4.22}$$

where $j = \sqrt{-1}$, $\mathscr{G}_1$ can be evaluated at the poles $s = m_B + \xi$ and $s = 0$ on the left of the contour $\mathscr{L}_1$, respectively

$$\mathscr{G}_1 \approx \mathrm{Res}[J_1(s), m_B + \xi] + \mathrm{Res}[J_1(s), 0], \tag{4.23}$$

where

$$\begin{aligned}&\mathrm{Res}[J_1(s), m_B + \xi] \\ &= -\lim_{s \to m_B + \xi}(s - m_B - \xi) J_1(s) \\ &= \frac{\Gamma(m_{B,s}+m_B)\Gamma(m_E + m_B + \xi)\Gamma(-m_B - \xi)}{\Gamma(1 - m_B - \xi)}\Gamma(m_{E,s} - m_B - \xi)\left(\frac{\lambda_E}{\lambda_B}\right)^{-(m_B+\xi)},\end{aligned} \tag{4.24a}$$

$$\mathrm{Res}[J_1(s), 0] = \Gamma(m_E)\Gamma(m_{E,s})\Gamma(m_{B,s} - \xi)\Gamma(m_B + \xi), \tag{4.24b}$$

subsequently, plugging the obtained results into (4.22) and then into (4.19), yields

$$\hat{I}_1 \approx \frac{\tau_1}{2\pi j}\int_{\mathscr{L}_2} \mathrm{Res}[J_1(s), m_B + \xi]\frac{\Gamma(1-\xi)\Gamma^2(\xi)}{\Gamma(1+\xi)\lambda_B^{\xi}} d\xi + \frac{\tau_1}{2\pi j}\int_{\mathscr{L}_2} \mathrm{Res}[J_1(s), 0]\frac{\Gamma(1-\xi)\Gamma^2(\xi)}{\Gamma(1+\xi)\lambda_B^{\xi}} d\xi, \tag{4.25}$$

where $\tau_1 = \frac{\mathscr{C}_B \Phi_E}{\lambda_B \ln(2)}$. After making some simple mathematical manipulations and applying the univariate Meijer's G-function, the proof of (4.21a) is obtained.

Regarding the proof for $\hat{I}_2$, it can be evaluated at the poles on the right of the contour $\mathscr{L}_1$, i.e., $s = m_{E,s} - \xi$ and $s = m_B$, and subsequently following the similar steps with (4.22)-(4.25), we obtain the asymptotic $\mathscr{I}_2$. □

4.7 Numerical Results and Conclusions

In order to confirm the accuracy of our derived analytical results given in Sections. 4.4, 4.5 and 4.6, Monte-Carlo simulations are therefore presented to compare with our analytical results given in (4.8a), (4.8b), (4.9), (4.12), and (4.13), respectively.

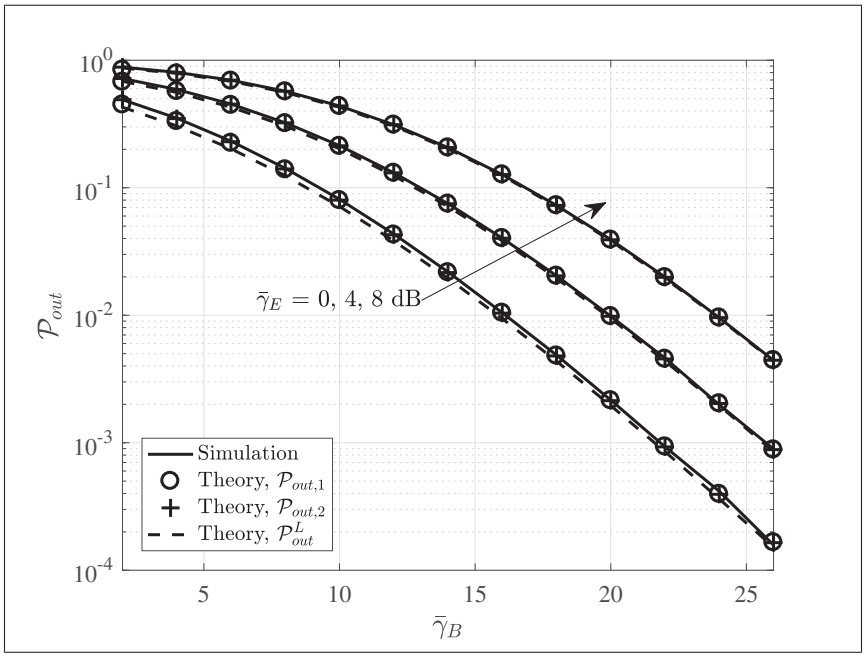


Figure 4.2 $\mathscr{P}_{out}$ versus $\bar{\gamma}_B$ over Fisher-Snedecor $\mathscr{F}$ fading channels when $R_t = 0.5$, $m_B = 2, m_E = 3$, $m_{s,B} = 2$, $m_{s,E} = 3$, and $\Omega_B = \Omega_E = 1$, respectively

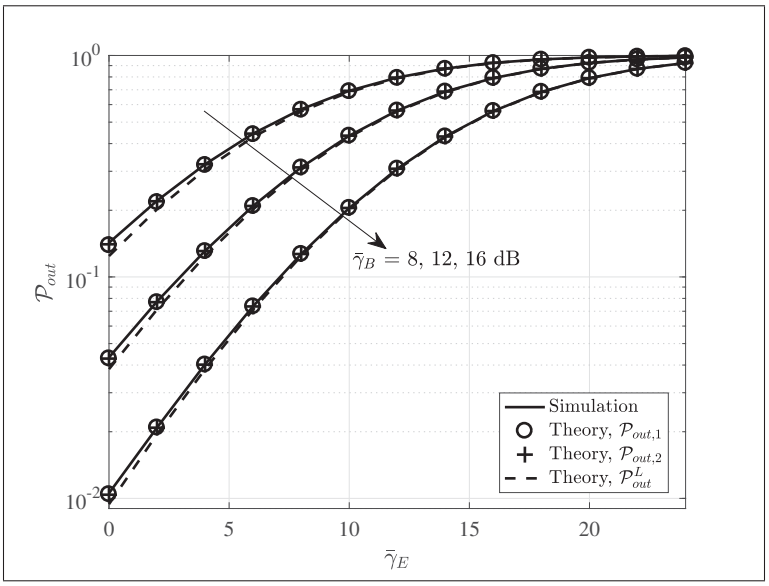


Figure 4.3 $\mathscr{P}_{out}$ versus $\bar{\gamma}_E$ over Fisher-Snedecor $\mathscr{F}$ fading channels when $R_t = 0.5$, $m_B = 2, m_E = 3$, $m_{s,B} = 2$, $m_{s,E} = 3$, and $\Omega_B = \Omega_E = 1$, respectively

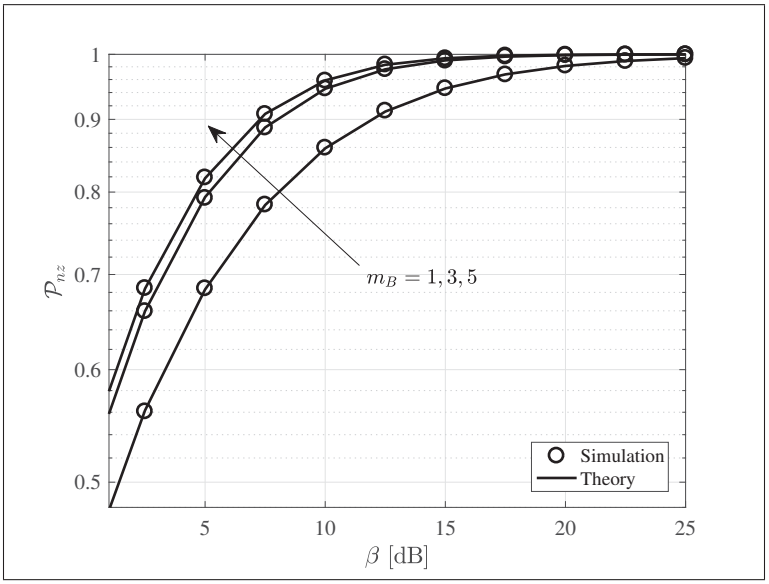


Figure 4.4 $\mathscr{P}_{nz}$ versus $\beta = \frac{\bar{\gamma}_B}{\bar{\gamma}_E}$ over Fisher-Snedecor $\mathscr{F}$ fading channels when $m_E = 3$, $m_{s,B} = 2$, $m_{s,E} = 2$, and $\Omega_B = \Omega_E = 1$, respectively

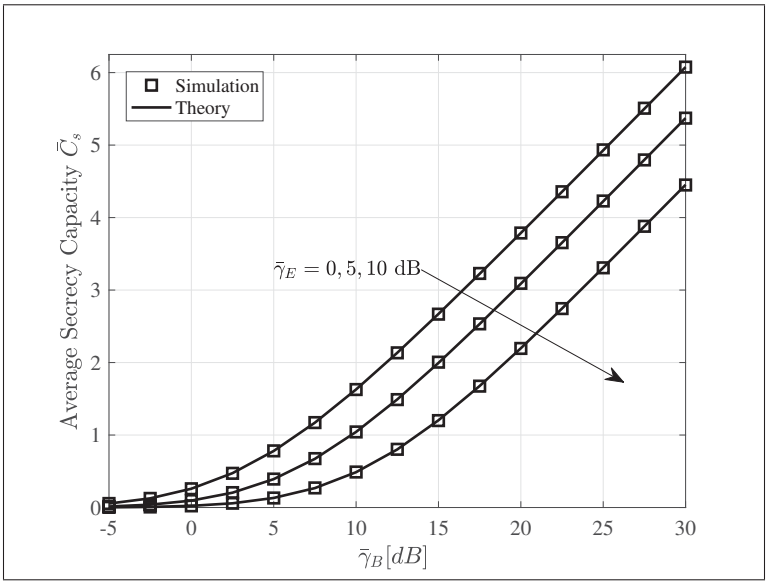


Figure 4.5 $\bar{C}_s$ versus $\bar{\gamma}_B$ over Fisher-Snedecor $\mathscr{F}$ fading channels when $m_B = m_{s,B} = 3$, $m_E = m_{s,E} = 2$, and $\Omega_B = \Omega_E = 1$, respectively

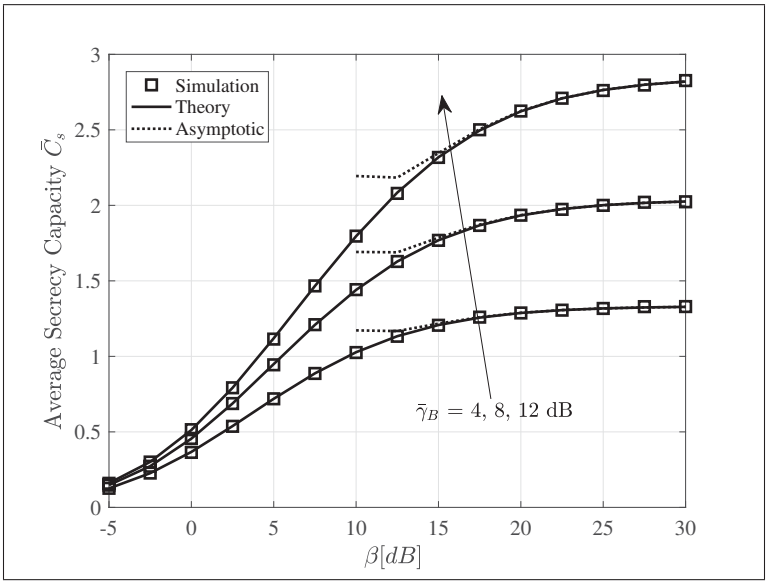


Figure 4.6 $\bar{C}_s$ versus β over Fisher-Snedecor $\mathscr{F}$ fading channels when $m_B = m_{s,B} = 3$, $m_E = m_{s,E} = 2$, and $\Omega_B = \Omega_E = 1$, respectively

Considering the active eavesdropping scenario, Figs. 4.2-4.4 verify the SOP and PNZ over the Fisher-Snedecor $\mathscr{F}$ fading channels. As observed from the three graphs, it is observed that our derivations are in good agreements with simulation outcomes. In addition, it is noteworthy to mention that the obtained two SOP expressions, given in (4.8a) and (4.8b), match well.

Moreover, the lower bound of SOP given in (4.9) both plotted in Figs. 4.2 and 4.3 demonstrates that the $\mathscr{P}_{out}^{L}$, as expected, is gradually approximating the exact SOP, especially as $\bar{\gamma}_E$ increases. Such a phenomenon is particularly vivid in Fig. 4.3. The lower bound of SOP is apparently beneficial because (i) when $\bar{\gamma}_E$ is at high signal-to-noise ratio (SNR) regime, it is highly tight to the exact SOP; (ii) it could offer a *simple and general* computational benchmark for wireless system designers when requiring quick evaluation of security risks.

In Fig. 4.4, we plot the PNZ against the ratio of $\bar{\gamma}_B$ and $\bar{\gamma}_E$ for selected values of m_B. One can obtain that larger value of m_B assures secure transmission with a higher probability. In other words, higher amount of shadowing of rms signal power is helpful to improve system secrecy. This is just the nature that how physical layer security deploys the randomness of wireless channels, i.e., fading, to enhance secrecy.

Figs. 4.5 and 4.6 illustrate the ASC against $\bar{\gamma}_B$ and β over the Fisher-Snedecor $\mathscr{F}$ wiretap fading channels, respectively. Apparently, our analytical result given by (4.13) is successfully confirmed by Monte-Carlo simulation outcomes. In addition, one can perceive the following conclusion: (i) higher $\bar{\gamma}_E$ leads to a lower ASC; (ii) the ASC can be improved by assuring high $\bar{\gamma}_B$; (iii) the ASC will reach a certain floor as β increases, as shown in Fig. 4.6; (iv) our asymptotic $\bar{C}_s$ given by (4.20) starts to gradually approach the exact one only when β is larger than 10 dB for our given simulation configuration.

4.8 Conclusions

In this paper, we have investigated the physical layer security over the Fisher-Snedecor $\mathscr{F}$ wiretap fading channels. The SOP, PNZ and ASC were derived with closed-form expressions, which are given in terms of Meijer's G-function. In addition, the asymptotic analysis of ASC

was further provided when the ratio between $\bar{\gamma}_B$ and $\bar{\gamma}_E$ is at high SNR regime. The accuracy of our analytical results were efficiently validated by Monte-Carlo simulation results.

CHAPTER 5

ON PHYSICAL LAYER SECURITY OVER FOX'S H-FUNCTION WIRETAP FADING CHANNELS

Long Kong[1], Georges Kaddoum[1], and Hatim Chergui[2]

[1]Département de Génie électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3
[2]National Institute of Telecommunications (INPT), Rabat, Morocco.

Paper published in *IEEE Transactions on Vehicular Technology*, May. 2019.

5.1 Abstract

Most of the well-known fading distributions, if not all of them, could be encompassed by the Fox's H-function fading. Consequently, we investigate the physical layer security (PLS) over Fox's H-function fading wiretap channels, in the presence of non-colluding and colluding eavesdroppers. In particular, for the non-colluding scenario, closed-form expressions are derived for the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), and the average secrecy capacity (ASC). These expressions are given in terms of either univariate or bivariate Fox's H-function. In order to show the effectiveness of our derivations, three metrics are respectively listed over the following frequently used fading channels, including Rayleigh, Weibull, Nakagami-m, $\alpha-\mu$, Fisher-Snedecor (F-S) $\mathscr{F}$, and extended generalized-$\mathscr{K}$ (EGK). Our tractable results are not only straightforward and general, but also feasible and applicable, especially the SOP, which is usually limited to the lower bound in the literature due to the difficulty of deriving closed-from analytical expressions. For the colluding scenario, a super eavesdropper equipped with maximal ratio combining (MRC) or selection-combining (SC) schemes is characterized. The lower bound of SOP and exact PNZ are thereafter derived with closed-form expressions in terms of the multivariate Fox's H-function. In order to validate the accuracy of our analytical results, Monte-Carlo simulations are subsequently conducted for the aforementioned fading channels. One can observe that for the former non-colluding scenario, we have perfect agreement between the exact analytical and simula-

tion results, and highly accurate approximations between the exact and asymptotic analytical results. On the contrary, the SOP and PNZ of colluding eavesdropper is greatly degraded with the increase of the number of eavesdroppers. Also, the so-called super eavesdropper with MRC is much powerful to wiretap the main channel than the one with SC.

Keywords: Physical layer security, Fox's H-function wiretap fading channels, Mellin transform, secrecy outage probability, probability of non-zero secrecy capacity, average secrecy capacity.

5.2 Introduction

Different wireless systems are usually characterized with various statistical models. For example, the gamma-gamma distribution was introduced to model the free space optical (FSO) communication link Lei, H., Dai, Z., Ansari, I. S., Park, K. H., Pan, G. & Alouini, M. S. (2017b); Lei, H., Luo, H., Park, K. H., Ren, Z., Pan, G. & Alouini, M. S. (2018a), and Fisher-Snedecor (F-S) $\mathscr{F}$ to model the device-to-device communication Badarneh *et al.* (2018); Yoo *et al.* (2017). As such, many endeavors have been drawn to investigate the mathematical characteristics of secure transmission for different communication scenarios.

Dating back to the fundamental works of physical layer security (PLS) from the information theoretical perspective, Shannon and Wyner are undoubtedly the pioneers in this field Shannon (1949); Wyner (1975). They established the mathematical background of perfect secrecy and wiretap channel models. Later on, Wyner's classic wiretap model was investigated over additive white Gaussian noise channel (AWGN) and Rayleigh fading channels Bloch *et al.* (2008); Leung-Yan-Cheong & Hellman (1978). Over the past decades, plenty of research efforts have been pursued on the investigation of PLS over various fading channels, such as Rayleigh Bloch *et al.* (2008), Rician Ai , Y., Kong, L. & Cheffena, M. (2019); Liu (2013a), Nakagami-m, Weibull Liu (2013b), Lognormal Pan, G., Tang, C., Zhang, X., Li, T., Weng, Y. & Chen, Y. (2016), generalized-$\mathscr{K}$ Kong & Kaddoum (2019); Lei *et al.* (2016a,1,1); Wu *et al.* (2018a), and $\alpha-\mu$ (or, equivalently, generalized gamma) Kong *et al.* (2016b,1,1,1); Lei *et al.* (2015,1),

$\alpha-\eta-\kappa-\mu$ Mathur, A., Ai, Y., Bhatnagar, M. R., Cheffena, M. & Ohtsuki, T. (2018), etc. Secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), and the average secrecy capacity (ASC) are the three typical and frequently studied secrecy metrics.

As more new communication topologies appear, e.g., device-to-device (D2D) communications, FSO communications, intervehicle communication, millimeterwave (mmWave) communications, wireless body area networks (WBAN), and cognitive radios, the existing models become obsolete. As such, more advanced and better suited fading models were subsequently proposed and analyzed, such as $\alpha-\mu$ Yacoub (2007a), $\kappa-\mu/\eta-\mu$ Yacoub, M. D. (2007b), F-S $\mathscr{F}$ Badarneh *et al.* (2018); Yoo *et al.* (2017), the extended generalized-$\mathscr{K}$ (EGK) Yilmaz, F. & Alouini, M. S. (2012), cascaded $\alpha-\mu$ fading Kong *et al.* (2018a), among many other fading channels.

With the emergence of various fading models, a unified and generic fading model is required to subsume most, if not all, of these fading distributions. Fox's H-function distribution, reported in Alhennawi *et al.* (2016); Ayadi, M. M. H. E., Ismail, M. H. & Alhennawi, H. R. (2016); Rahama, Y. A., Ismail, M. H. & Hassan, M. S. (2016), is one possible model to accommodate various fading models with high flexibility. It was first introduced in Bodenschatz (1992) and Cook Jr (1981) as a pure mathematical finding, and can be generalized to the Gamma, exponential, Chi-square, Weibull, Rayleigh, Half-Normal distribution, etc. Other examples, including generalized-$\mathscr{K}$, $\alpha-\mu$, F-S $\mathscr{F}$, and EGK, were recently explored by Alhennawi *et al.* Alhennawi *et al.* (2016) and Rahama *et al.* Rahama *et al.* (2018). These findings were achieved by transforming these probability density distributions (PDFs) of received signal-to-noise ratios (SNRs) in terms of Fox's H-function.

The feasibility and applicability of Fox's H-function distribution as a general fading model for wireless communication is not new. In Yilmaz & Alouini (2012), a variation of Fox's H-function fading model was proposed as a general model for most well-known distributions. Jeong *et al.* found that Fox's H-function distribution offers a better fading model of vehicle-to-vehicle (V2V) communication than other ordinary fading distributions Jeong *et al.* (2013).

More recently, Alhennawi *et al.* in Alhennawi *et al.* (2016) derived the symbol error rate (SER) and channel capacity of single- and multiple-branch diversity receivers when communicating over Fox's H-function fading channels. As a consequence, the advantages of Fox's H-function fading are threefold:

- The genericity of its form for most distribution, e.g., Rayleigh, Nakagami-m, Weibull, $\alpha - \mu$, etc;
- The simplicity and the generality of it to derive the key performance metrics of wireless communications systems, e.g., outage probability, SER, and channel capacity Alhennawi *et al.* (2016).
- The possibility of using its distribution to study the PLS analysis over $\alpha - \mu$, F-S $\mathscr{F}$ fading channels Kong & Kaddoum (2018); Kong *et al.* (2018a,1); Lei *et al.* (2017a).

To the best of the authors' knowledge, apart from the investigation of PLS over the aforementioned fading channels Ai *et al.* (2019); Bloch *et al.* (2008); Kong & Kaddoum (2019); Kong *et al.* (2016b,1,1); Lei *et al.* (2015,1,1,1,1); Liu (2013a,1); Pan *et al.* (2016); Wu *et al.* (2018a), including generalized-$\mathscr{K}$, $\alpha - \mu$, $\kappa - \mu$ Bhargav, N., Cotton, S. L. & Simmons, D. E. (2016); Iwata, S., Ohtsuki, T. & Kam, P. Y. (2017); Moualeu & Hamouda (2017), F-S $\mathscr{F}$ Kong & Kaddoum (2018), no works has ever been found to analyze the PLS over the general Fox's H-function fading channels. To this end, this paper is subject to the investigation of PLS over Fox's H-function fading channels, with consideration of the non-colluding and colluding eavesdropping scenarios.

5.2.1 Our Work and Contributions

The contributions of this paper are multifold, which are listed as follows:

1) Novel exact and closed-form expressions are initially derived for the secrecy metrics, including the SOP, PNZ, and ASC. Our formulations, in terms of univariate or bivariate Fox's H-function, are given in *simple* and *tractable* mathematical expressions.

2) The difficulty of deriving closed-form expressions for the SOP explicitly lies in tractable integrals. Consequently, many works can be found on the development of lower bound of the SOP ($\mathscr{P}_{out} = Pr(C_s \geq R_s)$). Since the lower bound of SOP is actually the complementary of the probability of non-zero secrecy capacity, i.e., $\mathscr{P}_{nz} = Pr(C_s > 0)$, it is much easier to obtain the lower bound of the SOP and PNZ, which can be found in Yacoub (2007a). Strictly speaking, our work fills this gap of lacking exact closed-form SOP expressions.

3) The obtained general and unified secrecy metrics' expressions are found identical with the existing works when being compared with Monte-Carlo simulation results. Moreover, the obtained secrecy expressions can be straightforward applied to other transformable but not listed herein wiretap fading channels.

4) The asymptotic behaviors of these secrecy metrics are also obtained for the sake of providing simple but highly accurate approximations of secrecy metrics at high average signal-to-noise (SNR) regime.

5) Considering the colluding eavesdropping scenario with maximal ratio combining (MRC) and selection combining (SC) schemes, the lower bound of the SOP and exact PNZ are characterized in terms of multivariate Fox's H-function.

Resultantly, the obtained analytical results are especially beneficial since the analytical expressions themselves (i) provide a unified approach to analyze the PLS over a generalized fading model; (ii) serve as an efficient and convenient tool to validate and compare the special cases of Fox's H-function fading channels; and (iii) enable researchers and wireless communication engineers to quickly evaluate secrecy performance when encountering security risks.

5.2.2 Structure and Notations

The rest of this paper is structured as follows: Section 5.3 illustrates Fox's H-function fading and its Mellin transform. In Section 5.4, the system model and problem formulation are presented. In the presence of non-colluding and colluding scenarios, secrecy analysis are respectively conducted in Sections 5.5, 5.6, and 5.7, together with several examples. Afterwards,

in Section 5.8, numerical results and discussions are presented. Finally, Section 5.9 concludes the paper.

Mathematical Functions and Notations: $j \triangleq \sqrt{-1}$, $\Gamma(.)$ is the complete Gamma function, $H_{p,q}^{m,n}[.]$ is the univariate Fox's H-function (Mathai, A. M., Saxena, R. K. & Haubold, H. J., 2009b, eq. (1.2)), $H_{p,q;p_1,q_1;p_2,q_2}^{m,n;m_1,n_1;m_2,n_2}$ is the extended generalized bivariate Fox's H-function (Mathai *et al.*, 2009b, eq. (2.56)). $H_{p,q;p_1,q_1;\cdots;p_L,q_L}^{m,n;m_1,n_1;\cdots;m_L,n_L}$ is the multivariate Fox's H-function (Mathai *et al.*, 2009b, eq. (2.56)). $f(x)$ and $F(x)$ represent the probability density function (PDF) and cumulative distribution function (CDF) of x, respectively. $\mathscr{B}(x,y)$ is the Beta function (Gradshteyn & Ryzhik, 2014, eq. (8.380.1)). $\mathscr{M}[f(x),s]$ denotes the Mellin transform of $f(x)$. Res$[f(x),s]$ represents the residue of function $f(x)$ at pole $x=p$. $\Psi_0(\cdot)$ is the digamma function.

5.3 Preliminary

5.3.1 Fox's H-Function Fading

Consider a wireless communication link over a fading channel, where the instantaneous SNR at user k, γ_k, follows Fox's H-function PDF, given by Bodenschatz (1992)

$$f_k(\gamma_k) = \kappa H_{p,q}^{m,n}\left[\lambda\gamma_k \left| \begin{matrix}(a_i,A_i)_{i=1:p}\\(b_l,B_l)_{l=1:q}\end{matrix}\right.\right] \overset{(a)}{=} \frac{\kappa}{2\pi j}\int_{\mathscr{L}} \Theta_k(s)(\lambda\gamma_k)^{-s}ds, \quad \gamma>0, \tag{5.1}$$

where $\lambda > 0$ and κ are constants such that $\int_0^\infty f_k(\gamma_k)d\gamma_k = 1$. $(x_i,y_i)_l$ is a shorthand for $(x_1,y_1),\cdots,(x_l,y_l)$. Step (a) is developed by expressing Fox's H-function in terms of its definition (Mathai *et al.*, 2009b, eq. (1.2)). $A_i > 0$ for all $i = 1,\cdots,p$, and $B_l > 0$ for all $l = 1,\cdots,q$. $0 \le m \le q$, $0 \le n \le p$, $\mathscr{L}$ is a suitable contour separating the poles of the gamma functions

$\Gamma(b_l + B_l s)$ from the poles of the gamma functions $\Gamma(1 - a_i - A_i s)$,

$$\Theta_k(s) = \frac{\prod_{l=1}^{m} \Gamma(b_l + B_l s) \prod_{i=1}^{n} \Gamma(1 - a_i - A_i s)}{\prod_{l=m+1}^{q} \Gamma(1 - b_l - B_l s) \prod_{i=n+1}^{p} \Gamma(a_i + A_i s)}. \tag{5.2}$$

The cumulative distribution function (CDF) of the received SNR at user k, i.e., γ_k is given by (Bodenschatz, 1992, eqs. (3.9) and (3.7))

$$F_k(\gamma_k) = \frac{\kappa}{\lambda} H_{p+1,q+1}^{m,n+1} \left[\lambda \gamma_k \middle| \begin{matrix} (1,1), (a_i + A_i, A_i)_p \\ (b_l + B_l, B_l)_q, (0,1) \end{matrix} \right], \tag{5.3a}$$

or

$$F_k(\gamma_k) = 1 - \frac{\kappa}{\lambda} H_{p+1,q+1}^{m+1,n} \left[\lambda \gamma_k \middle| \begin{matrix} (a_i + A_i, A_i)_p, (1,1) \\ (0,1), (b_l + B_l, B_l)_q \end{matrix} \right] = 1 - \bar{F}_k(\gamma_k), \tag{5.3b}$$

where $\bar{F}_k(\gamma)$ is the complementary CDF (CCDF). For the notational convenience, Θ_k^f and Θ_k^F are used thereafter to denote the PDF and CDF of Fox's H-function, respectively. The Mellin transform of $f_k(\gamma)$ is defined and given as (Alhennawi *et al.*, 2016, eq. (5)) (Mathai *et al.*, 2009b, eq. (2.8)),

$$\mathscr{M}[f_k(\gamma_k), s] = \int_0^\infty f_k(\gamma_k) \gamma^{s-1} d\gamma_k = \kappa \lambda^{-s} \Theta_k(s). \tag{5.4}$$

5.3.2 Special Cases

As mentioned before, Fox's H-function distribution provides enough flexibility to accommodate most fading distributions. As a result, the objective herein is to list some well-known examples, such as the $\alpha - \mu$[1], F-S $\mathscr{F}$, and EGK, as shown in Table. 5.1, where $\bar{\gamma}_k$ is the average received SNR at user k.

[1] Since $\alpha - \mu$ distributions can be attributed to exponential, one-sided Gaussian, Rayleigh, Nakagami-m, Weibull and Gamma fading distributions by assigning specific values for α and μ, respectively Yacoub (2007a), secrecy analysis on these fading distributions is thus omitted herein.

Table 5.1 Exact expressions of $f_k(\gamma_k)$ for different special cases of Fox's H-function distribution

Instantaneous SNR	$f_k(\gamma_k)$
$\alpha-\mu$ (Yilmaz & Alouini, 2012, Tab. V)	$f_k(\gamma_k)=\kappa H_{0,1}^{1,0}\left[\lambda\gamma_k\middle\vert\begin{matrix}-\\(\mu-\frac{1}{\alpha},\frac{1}{\alpha})\end{matrix}\right]$, where $\kappa=\frac{\beta}{\Gamma(\mu)\bar{\gamma}_k},\lambda=\frac{\beta}{\bar{\gamma}_k},\beta=\frac{\Gamma\left(\mu+\frac{1}{\alpha}\right)}{\Gamma(\mu)}$.
F-S $\mathscr{F}$ (Yoo *et al.*, 2017, eq. (5))	$f_k(\gamma_k)=\kappa H_{1,1}^{1,1}\left[\lambda\gamma_k\middle\vert\begin{matrix}(-m_{k,s},1)\\(m_k-1,1)\end{matrix}\right]$, where $\kappa=\frac{\lambda}{\Gamma(m_k)\Gamma(m_{k,s})},\lambda=\frac{m_k}{m_{k,s}\bar{\gamma}_k}$.
EGK (Rahama *et al.*, 2018, eq. (18))	$f_k(\gamma_k)=\kappa H_{0,2}^{2,0}\left[\lambda\gamma_k\middle\vert\begin{matrix}-\\(m_l-\frac{1}{\xi_l},\frac{1}{\xi_l}),(m_{sl}-\frac{1}{\xi_{sl}},\frac{1}{\xi_{sl}})\end{matrix}\right]$, where $\kappa=\frac{\beta_l\beta_{sl}}{\Gamma(m_l)\Gamma(m_{sl})\bar{\gamma}_k},\lambda=\frac{\beta_l\beta_{sl}}{\bar{\gamma}_k},\beta_l=\frac{\Gamma\left(m_l+\frac{1}{\xi_l}\right)}{\Gamma(m_l)}$, and $\beta_{sl}=\frac{\Gamma\left(m_{sl}+\frac{1}{\xi_{sl}}\right)}{\Gamma(m_{sl})}$.

5.4 System Model and Problem Formulation

5.4.1 System Model

The Alice-Bob-Eve classic wiretap model is used here to illustrate a legitimate transmission link (Alice $\rightarrow$ Bob) in the presence of a malicious eavesdropper. In such a wiretap channel model, the transmitter Alice (A) wishes to send secret messages to the intended receiver Bob (B) in the presence of an eavesdropper Eve (E); the link between A and B is called the main channel, whereas the one between A and E is named as the wiretap channel. It is assumed that (i) all users are equipped with a single antenna; (ii) both links are independent and subjected to Fox's H-function fading; and (iii) a perfect channel state information (CSI) is available at all users.

As a result, the received SNRs at B and E are denoted as $\gamma_k, k \in \{B,E\}$, which follow Fox's H-function PDF, and are respectively given by

$$f_B(\gamma_B) = \kappa_B H_{p_0,q_0}^{m_0,n_0}\left[\lambda_B\gamma_B \left| \begin{matrix}(a_i,A_i)_{i=1:p_0}\\(b_l,B_l)_{l=1:q_0}\end{matrix}\right.\right],\ \gamma_B > 0, \tag{5.5a}$$

$$f_E(\gamma_E) = \kappa_E H_{p_1,q_1}^{m_1,n_1}\left[\lambda_E\gamma_E \left| \begin{matrix}(c_i,C_i)_{i=1:p_1}\\(d_l,D_l)_{l=1:q_1}\end{matrix}\right.\right],\ \gamma_E > 0. \tag{5.5b}$$

5.4.2 Problem Formulation

According to Bloch *et al.* (2008), the secrecy capacity over fading wiretap channels is defined as the difference between the main channel capacity $C_M = \log_2(1+\gamma_B)$ and the wiretap channel capacity $C_W = \log_2(1+\gamma_E)$ as follows

$$C_s = \begin{cases} C_M - C_W, & \gamma_B > \gamma_E \\ 0, & \text{otherwise.} \end{cases} \tag{5.6}$$

In other words, a positive secrecy capacity can be assured if and only if the received SNR at Bob has a superior quality than that at Eve's.

5.4.2.1 Secrecy Outage Probability

The outage probability of the secrecy capacity is defined as the probability that the secrecy capacity C_s falls below the target secrecy rate R_t, i.e.,

$$\mathscr{P}_{out}(R_s) = Pr(C_s < R_t). \tag{5.7}$$

Technically speaking, SOP can be conceptually explained as two cases: (i) $C_s < R_t$ whilst positive secrecy capacity is surely guaranteed; (ii) secrecy outage definitely happens when C_S

is non-positive. To this end, (A V-17) can be rewritten as follows Kong *et al.* (2016a); Lei *et al.* (2016b),

$$\mathscr{P}_{out}(R_s) = \mathscr{P}r(\gamma_B \leq R_s\gamma_E + R_s - 1) = \int_0^{\infty} F_B(\gamma_0) f_E(\gamma_E) d\gamma_E, \tag{5.8}$$

where $R_s = 2^{R_t}$, $\gamma_0 = R_s\gamma_E + \mathscr{W}$, and $\mathscr{W} = R_s - 1$.

The SOP characterizes the probability of failure to achieve a reliable and secure transmission. In addition, it shows that PLS can be achieved by fading alone, even when Eve has a better average SNR than Bob.

5.4.2.2 Probability of Non-Zero Secrecy Capacity

The PNZ refers to the event that the positive secrecy capacity can be surely achieved, namely $Pr(C_s > 0)$, thus respecting its definition, (5.6) can be further rewritten as follows,

$$\mathscr{P}_{nz} = Pr(\gamma_B > \gamma_E) = \int_0^{\infty} f_B(\gamma_B) F_E(\gamma_B) d\gamma_B. \tag{5.9}$$

5.4.2.3 Average Secrecy Capacity

average secrecy capacity provides a mathematical indicator of the capacity limit for a given constraint of perfect secrecy.

By using some simple mathematical manipulations, the ASC can be further re-expressed as the sum of three terms, which are given by Lei *et al.* (2016c)

$$\begin{aligned} \bar{C}_s = &\underbrace{\int_0^{\infty} \log_2(1+\gamma_B) f_B(\gamma_B) F_E(\gamma_B) d\gamma_B}_{I_1} + \underbrace{\int_0^{\infty} \log_2(1+\gamma_E) f_E(\gamma_E) F_B(\gamma_E) d\gamma_E}_{I_2} \\ &- \underbrace{\int_0^{\infty} \log_2(1+\gamma_E) f_E(\gamma_E) d\gamma_E}_{I_3}. \end{aligned} \tag{5.10}$$

For the brevity of the following derivations, let $g_k(\gamma_k) = \ln(1+\gamma_k) f_B(\gamma_k)$.

5.5 Secrecy Metrics Characterization

To begin the characterization of the secrecy performance over Fox's H-function fading channels, one useful and unified theorem is first provided. This theorem is essentially beneficial to the acquisition of the final closed-form expressions for the aforementioned three secrecy metrics.

Theorem 3. *Consider a general fading channel where the received SNR's PDF is $f(\gamma)$ and another function $u(\gamma)$. Suppose their Mellin transforms are $\mathscr{M}[f(\gamma), s]$ and $\mathscr{M}[u(\gamma), s]$, respectively. If the Mellin transform of $u(\gamma)$ exists, then by using Parseval's formula for Mellin transform (Debnath & Bhatta, 2014, eq. (8.3.23)), we have*

$$\int_0^\infty f(\gamma) u(\gamma) d\gamma = \frac{1}{2\pi j} \int_{\mathscr{L}} \mathscr{M}[f(\gamma), s] \mathscr{M}[u(\gamma), 1-s] ds, \tag{5.11}$$

where $\mathscr{L}$ is the integration path from $\upsilon - j\infty$ to $\upsilon + j\infty$, and υ is a constant.

The aforementioned Theorem is recalled to make a basis for the following derivations. To this end, we have the following remark.

Remark 5. *The SOP, PNZ, and ASC over Fox's H-function fading wiretap channels are respectively given by*

$$\mathscr{P}_{out} = \frac{1}{2\pi j} \int_{\mathscr{L}_1} \mathscr{M}[F_B(\gamma_0), 1-s] \mathscr{M}[f_E(\gamma_E), s] ds, \tag{5.12a}$$

$$\mathscr{P}_{nz} = \frac{1}{2\pi j} \int_{\mathscr{L}_1} \mathscr{M}[F_E(\gamma_B), 1-s] \mathscr{M}[f_B(\gamma_B), s] ds, \tag{5.12b}$$

$$\begin{aligned} \bar{C}_s = & \frac{1}{2\pi j} \int_{\mathscr{L}_1} \mathscr{M}[g_B(\gamma_E), 1-s] \mathscr{M}[F_E(\gamma_B), s] ds \\ & + \frac{1}{2\pi j} \int_{\mathscr{L}_1} \mathscr{M}[g_E(\gamma_E), 1-s] \mathscr{M}[F_B(\gamma_E), s] ds \\ & - \frac{1}{2\pi j} \int_{\mathscr{L}_1} \mathscr{M}[f_E(\gamma_E), 1-s] \mathscr{M}[\ln(1+\gamma_E), s] ds \end{aligned} \tag{5.12c}$$

Proof. Recalling (A V-18), (5.9), and (5.10), and then using **Theorem** 3, the proofs for (5.12a), (5.12b), and (5.12c) are directly accomplished. □

5.5.1 SOP Characterization

5.5.1.1 Exact SOP Characterization

Theorem 4. *The SOP over Fox's H-function fading wiretap channels is given by (5.13),*

$$\mathscr{P}_{out} = 1 - \frac{\kappa_B \kappa_E \mathscr{W}}{\lambda_B R_s} H_{1,0:q_1,p_1+1:q_0,p_0+1}^{0,1:n_1+1,m_1:n_0,m_0} \left[\frac{R_s}{\lambda_E \mathscr{W}}, \frac{1}{\lambda_B \mathscr{W}} \middle| \begin{matrix} (2,1,1) & (1-d_l, D_l)_{l=1:q_1} & (1-b_l-B_l, B_l)_{l=1:q_0} \\ - & (1,1),(1-c_i,C_i)_{i=1:p_1} & (1-a_i-A_i, A_i)_{i=1:p_0},(0,1) \end{matrix} \right], \tag{5.13}$$

Proof. See Appendix II.1. □

5.5.1.2 Lower Bound of SOP

As $\bar{\gamma}_B$ and $\bar{\gamma}_E$ tend to ∞, we have

$$\mathscr{P}_{out} = Pr\left(\log_2 \left(\frac{1+\gamma_B}{1+\gamma_E} \right) < R_t \right) \approx \underbrace{Pr\left(\log_2 \left(\frac{\gamma_B}{\gamma_E} \right) < R_t \right)}_{\mathscr{P}_{out}^L} = \int_0^\infty F_B(R_s y) f_E(y) dy. \tag{5.14}$$

Proposition 4. *As $\bar{\gamma}_B$ and $\bar{\gamma}_E$ tend to ∞, the lower bound of the SOP over Fox's H-function fading channels is given by*

$$\mathscr{P}_{out}^L = 1 - \frac{\kappa_B \kappa_E}{\lambda_B \lambda_E} H_{p_1+q_2+1,q_1+p_2+1}^{m_1+n_2+1,n_1+m_2} \left[\frac{\lambda_B R_s}{\lambda_E} \middle| \begin{matrix} (a_i+A_i, A_i)_{i=1:n_1}, (1-d_l-D_l, D_l)_{l=1:q_2}, (a_i+A_i, A_i)_{i=n_1+:p_1}, (1,1) \\ (0,1), (b_l+B_l, B_l)_{l=1:m_1}, (1-c_i-C_i, C_i)_{i=1:p_2}, (b_l+B_l, B_l)_{l=m_1+1:q_1} \end{matrix} \right]. \tag{5.15}$$

Proof. By applying the Mellin transform of the product of two Fox's H-function (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), the proof is accomplished. □

5.5.2 PNZ Characterization

Theorem 5. *The PNZ over Fox's H-function wiretap fading channels is given by (5.16),*

$$\mathscr{P}_{nz} = \frac{\kappa_B \kappa_E}{\lambda_B \lambda_E} H^{m_1+n_0,n_1+m_0+1}_{p_0+q_1+1,q_0+p_1+1}\left[\frac{\lambda_E}{\lambda_B}\middle|\begin{matrix}(1,1),(c_i+C_i,C_i)_{i=1:p_1},(1-b_l-B_l,B_l)_{l=1:q_0},(c_i+C_i,C_i)_{i=n_1+1:p_1}\\(d_l+D_l,D_l)_{l=1:m_1},(1-a_i-A_i,A_i)_{i=1:p_0},(0,1),(d_l+D_l,D_l)_{l=m_1+1:q_1}\end{matrix}\right]. \tag{5.16}$$

Proof. According to (5.12b), $\mathscr{M}[F_E(\gamma_B),1-s]$ and $\mathscr{M}[f_B(\gamma_B),s]$ are separately given by

$$\mathscr{M}[F_E(\gamma_B),1-s] = \frac{\kappa_E}{\lambda_E^{2-s}}\Theta_E^F(1-s), \tag{5.17a}$$

$$\mathscr{M}[f_B(\gamma_B),s] = \frac{\kappa_B}{\lambda_B^{s}}\Theta_B^f(s). \tag{5.17b}$$

Next, substituting (5.17a) and (5.17b) into (5.12b), yields the following result

$$\mathscr{P}_{nz} = \frac{\kappa_B \kappa_E}{2\lambda_E^2 \pi j}\int_{\mathscr{L}_1}\Theta_B^f(s)\Theta_E^F(1-s)\left(\frac{\lambda_B}{\lambda_E}\right)^{-s} ds, \tag{5.18}$$

Subsequently, directly applying the definition of univariate Fox's H-function, the proof is achieved.

Alternatively, we provide another method to prove (5.16). Revisiting (5.9) and directly replacing $f_B(\gamma_B)$ and $F_E(\gamma_B)$ with their expressions, we have

$$\begin{aligned}\mathscr{P}_{nz} = \frac{\kappa_B \kappa_E}{\lambda_E} \int_0^{\infty} H_{p_0,q_0}^{m_0,n_0} \left[\lambda_B \gamma_B \middle| \begin{matrix} (a_i, A_i)_{i=1:p_0} \\ (b_l, B_l)_{l=1:q_0} \end{matrix} \right] \\ \times H_{p_1+1,q_1+1}^{m_1,n_1+1} \left[\lambda_E \gamma_B \middle| \begin{matrix} (1,1), (c_i + C_i, C_i)_{i=1:p_1} \\ (d_l + D_l, D_l)_{l=1:q_1}, (0,1) \end{matrix} \right] d\gamma_B,\end{aligned} \tag{5.19}$$

where the last step is derived by using the Mellin transform of the product of two Fox's H-function (Prudnikov *et al.*, 1990, eq. (2.25.1.1)). □

5.5.3 ASC Characterization

Theorem 6. *The ASC over Fox's H-function wiretap fading channels is given by*

$$\bar{C}_s = \frac{1}{\ln(2)} (I_1 + I_2 - I_3), \tag{5.20}$$

where I_1, I_2 and I_3 are respectively given by (5.21a), (5.21b) and (5.21c).

$$\begin{aligned}I_1 = &\frac{\kappa_B \kappa_E}{\lambda_B \lambda_E} \\ &\times H_{q_0,p_0:2,2:p_1+1,q_1+1}^{n_0,m_0:1,2:m_1,n_1+1} \left[\frac{1}{\lambda_B}, \frac{\lambda_E}{\lambda_B} \middle| \begin{matrix} (1 - b_l - B_l; B_l, B_l)_{l=1:q_0} \\ (1 - a_i - A_i; A_i, A_i)_{i=1:p_0} \end{matrix} \middle| \begin{matrix} (1,1), (1,1) \\ (1,1), (0,1) \end{matrix} \middle| \begin{matrix} (1,1), (c_i + C_i, C_i)_{i=1:q_1} \\ (d_l + D_l, D_l)_{l=1:p_1}, (0,1) \end{matrix} \right],\end{aligned} \tag{5.21a}$$

$$\begin{aligned}I_2 = &\frac{\kappa_B \kappa_E}{\lambda_B \lambda_E} \\ &\times H_{q_1,p_1:2,2:p_0+1,q_0+1}^{n_1,m_1:1,2:m_0,n_0+1} \left[\frac{1}{\lambda_E}, \frac{\lambda_B}{\lambda_E} \middle| \begin{matrix} (1 - d_l - D_l; D_l, D_l)_{l=1:q_1} \\ (1 - c_i - C_i; C_i, C_i)_{i=1:p_1} \end{matrix} \middle| \begin{matrix} (1,1), (1,1) \\ (1,1), (0,1) \end{matrix} \middle| \begin{matrix} (1,1), (a_i + A_i, A_i)_{i=1:p_0} \\ (b_l + B_l, B_l)_{l=1:q_0}, (0,1) \end{matrix} \right].\end{aligned} \tag{5.21b}$$

$$I_3 = \frac{\kappa_E}{\lambda_E} H_{q_1+2,p_1+2}^{n_1+1,m_1+2} \left[\frac{1}{\lambda_E} \middle| \begin{matrix} (1,1),(1,1),(1-d_l-D_l,D_l)_{l=1:p_1} \\ (1,1),(1-c_i-C_i,C_i)_{i=1:q_1},(0,1) \end{matrix} \right]. \tag{5.21c}$$

Proof. See Appendix II.2. □

5.5.4 Special Cases

Accommodating the closed-form expressions for secrecy performance metrics in the corresponding entries in Table 5.1, directly yields the results, as displayed in Tables 5.2 and 5.3. After some simple algebraic manipulations, one can observe the obtained results herein are consistent with the existing works Kong & Kaddoum (2018); Kong *et al.* (2018c); Lei *et al.* (2015,1).

5.6 Asymptotic Secrecy Metrics Characterization

The obtained secrecy expressions are given in terms of either univariate or bivariate Fox's H-function. In order to provide more insights at high or low SNR regime, the asymptotic behavior of the three aforementioned secrecy metrics are developed in this section.

According to Chergui *et al.* (2016), expansions of the univariate and bivariate Fox's H-functions can be derived by evaluating the residue of the corresponding integrands at the closest poles to the contour, namely, the minimum pole on the right for large Fox's H-function arguments and the maximum pole on the left for small ones.

5.6.1 Asymptotic SOP

The lower bound of the SOP is still expressed in terms of Fox's H-function, in order to study the asymptotic behavior of the SOP, the lower bound is further simplified by expanding the univariate Fox's H-function.

Table 5.2 Exact expressions of $\mathscr{P}_{out}$, $\mathscr{P}_{nz}$ and $\bar{C}_s$ for different special cases of Fox's H-function distribution

$\alpha-\mu$	$\mathscr{P}_{out} = 1-\frac{\kappa_B\kappa_E\mathscr{W}}{\lambda_B R_s}$ $\times H_{1,0:1,1:1,1}^{0,1:1,1:0,1}\left[\frac{R_s}{\lambda_E\mathscr{W}},\frac{1}{\lambda_B\mathscr{W}}\middle\vert \begin{matrix}(2,1,1)\\-\end{matrix}\middle\vert \begin{matrix}(1-\mu_E+\frac{1}{\alpha_E},\frac{1}{\alpha_E})\\(1,1)\end{matrix}\middle\vert \begin{matrix}(1-\mu_B,\frac{1}{\alpha_B})\\(0,1)\end{matrix}\right]$
	$\mathscr{P}_{nz} = \frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}H_{2,2}^{2,1}\left[\frac{\lambda_E}{\lambda_B}\middle\vert \begin{matrix}(1-\mu_B,\frac{1}{\alpha_B}),(1,1)\\(\mu_E,\frac{1}{\alpha_E}),(0,1)\end{matrix}\right]$
	$\bar{C}_s = \frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}H_{1,0:2,2:1,2}^{0,1:1,2:1,1}\left[\frac{1}{\lambda_B},\frac{\lambda_E}{\lambda_B}\middle\vert \begin{matrix}(1-\mu_B;\frac{1}{\alpha_B},\frac{1}{\alpha_B})\\-\end{matrix}\middle\vert \begin{matrix}(1,1),(1,1)\\(1,1),(0,1)\end{matrix}\middle\vert \begin{matrix}(1,1)\\(\mu_E,\frac{1}{\alpha_E}),(0,1)\end{matrix}\right]$ $+\frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}H_{1,0:2,2:1,2}^{0,1:1,2:1,1}\left[\frac{1}{\lambda_E},\frac{\lambda_B}{\lambda_E}\middle\vert \begin{matrix}(1-\mu_E;\frac{1}{\alpha_E},\frac{1}{\alpha_E})\\-\end{matrix}\middle\vert \begin{matrix}(1,1),(1,1)\\(1,1),(0,1)\end{matrix}\middle\vert \begin{matrix}(1,1)\\(\mu_B,\frac{1}{\alpha_B}),(0,1)\end{matrix}\right]$ $-\frac{\kappa_E}{\lambda_E}H_{3,2}^{1,3}\left[\frac{1}{\lambda_E}\middle\vert \begin{matrix}(1,1),(1,1),(1-\mu_E,\frac{1}{\alpha_E})\\(1,1),(0,1)\end{matrix}\right]$
F-S $\mathscr{F}$	$\mathscr{P}_{out} = 1-\frac{\kappa_B\kappa_E\mathscr{W}}{\lambda_B R_s}$ $\times H_{1,0:1,2:1,2}^{0,1:2,1:1,1}\left[\frac{R_s}{\lambda_E\mathscr{W}},\frac{1}{\lambda_B\mathscr{W}}\middle\vert \begin{matrix}(2,1,1)\\-\end{matrix}\middle\vert \begin{matrix}(2-m_E,1)\\(1,1),(1+m_{E,s},1)\end{matrix}\middle\vert \begin{matrix}(1-m_B,1)\\(m_{B,s},1),(0,1)\end{matrix}\right]$
	$\mathscr{P}_{nz} = \frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}H_{3,3}^{2,3}\left[\frac{\lambda_E}{\lambda_B}\middle\vert \begin{matrix}(1,1),(-m_{B,s},1),(1-m_E,1),(0,1)\\(m_E,1),(-1,1),(m_{E,s},1),(0,1)\end{matrix}\right]$
	$\bar{C}_s = \frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}H_{1,1:2,2:2,2}^{1,1:1,2:1,2}\left[\frac{1}{\lambda_B},\frac{\lambda_E}{\lambda_B}\middle\vert \begin{matrix}(m_B;1,1)\\(m_{B,s};1,1)\end{matrix}\middle\vert \begin{matrix}(1,1),(1,1)\\(1,1),(0,1)\end{matrix}\middle\vert \begin{matrix}(1,1),(1-m_{E,s},1)\\(m_E,1),(0,1)\end{matrix}\right]$ $+\frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}H_{1,1:2,2:2,2}^{1,1:1,2:1,2}\left[\frac{1}{\lambda_E},\frac{\lambda_B}{\lambda_E}\middle\vert \begin{matrix}(m_E;1,1)\\(m_{E,s};1,1)\end{matrix}\middle\vert \begin{matrix}(1,1),(1,1)\\(1,1),(0,1)\end{matrix}\middle\vert \begin{matrix}(1,1),(1-m_{E,s},1)\\(m_E,1),(0,1)\end{matrix}\right]$ $-\frac{\kappa_E}{\lambda_E}H_{3,3}^{2,3}\left[\frac{1}{\lambda_E}\middle\vert \begin{matrix}(1,1),(1,1),(1-m_E,1)\\(1,1),(m_{E,s},1),(0,1)\end{matrix}\right]$

Consequently, at high $\bar{\gamma}_B$ regime, we have $\frac{1}{\lambda_B}\to\infty$. By using the expanding rule, the asymptotic SOP is given by (5.22)

$$\begin{aligned}\mathscr{P}_{out}^{L} \approx & 1-\frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}\frac{\Gamma(\tau)\prod_{l=1,l\neq g}^{m_0}\Gamma(b_l+B_l+B_l\tau)\prod_{i=1}^{n_1}\Gamma(1-c_i-C_i+C_i\tau)}{\Gamma(1+\tau)\prod_{l=m_0+1}^{q_0}\Gamma(1-b_l-B_l-B_l\tau)\prod_{i=n_0+1}^{p_0}\Gamma(a_i+A_i+A_i\tau)}\\ & \times\frac{\prod_{i=1}^{n_0}\Gamma(1-a_i-A_i+A_i\tau)\prod_{l=1}^{m_1}\Gamma(d_l+D_l-D_l\tau)}{\prod_{i=n_1+1}^{p_2}\Gamma(c_i+C_i-C_i\tau)\prod_{l=m_1+1}^{q_1}\Gamma(1-d_l-D_l+D_l\tau)}\left(\frac{\lambda_E}{\lambda_B R_s}\right)^{\tau},\end{aligned} \tag{5.22}$$

$$\text{where } \tau=\max_{l=1:m_0}\left(-\frac{b_l+B_l}{B_l}\right), g=\operatorname*{argmax}_{l=1:m_0}\left(-\frac{b_l+B_l}{B_l}\right).$$

Table 5.3 Exact expressions of $\mathscr{P}_{out}$, $\mathscr{P}_{nz}$ and $\bar{C}_s$ for different special cases of Fox's H-function distribution

EGK	$\mathscr{P}_{out} = 1 - \frac{\kappa_B \kappa_E \mathscr{W}}{\lambda_B R_s}$ $\times H_{1,0:2,1:2,1}^{0,1:1,1:0,2}\left[\frac{R_s}{\lambda_E \mathscr{W}}, \frac{1}{\mathscr{W}\lambda_B}\middle\vert \begin{matrix}(2,1,1)\\ -\end{matrix}\middle\vert \begin{matrix}(1-m_E+\frac{1}{\xi_E},\frac{1}{\xi_E}),(1-m_{sE}+\frac{1}{\xi_{sE}},\frac{1}{\xi_{sE}})\\ (1,1)\end{matrix}\middle\vert \begin{matrix}(1-m_B,\frac{1}{\xi_B}),(1-m_{sB},\frac{1}{\xi_{sB}})\\ (0,1)\end{matrix}\right]$
	$\mathscr{P}_{nz} = \frac{\kappa_B \kappa_E}{\lambda_B \lambda_E} H_{3,3}^{2,3}\left[\frac{\lambda_E}{\lambda_B}\middle\vert \begin{matrix}(1,1),(1-m_B,\frac{1}{\xi_B}),(1-m_{sB},\frac{1}{\xi_{sB}})\\ (m_E,\frac{1}{\xi_E}),(m_{sE},\frac{1}{\xi_{sE}}),(0,1)\end{matrix}\right]$
	$\bar{C}_s = \frac{\kappa_B \kappa_E}{\lambda_B \lambda_E} H_{2,0:2,2:1,3}^{0,2:1,2:3,0}\left[\frac{1}{\lambda_B},\frac{\lambda_E}{\lambda_B}\middle\vert \begin{matrix}(1-m_B;\frac{1}{\xi_B},\frac{1}{\xi_B}),(1-m_{sB},\frac{1}{\xi_{sB}},\frac{1}{\xi_{sB}})\\ -\end{matrix}\middle\vert \begin{matrix}(1,1),(1,1)\\ (1,1),(0,1)\end{matrix}\middle\vert \begin{matrix}(1,1)\\ (m_E,\frac{1}{\xi_E}),(m_{sE},\frac{1}{\xi_{sE}}),(0,1)\end{matrix}\right]$
	$+\frac{\kappa_B \kappa_E}{\lambda_B \lambda_E} H_{2,0:2,2:1,3}^{0,2:1,2:3,0}\left[\frac{1}{\lambda_E},\frac{\lambda_B}{\lambda_E}\middle\vert \begin{matrix}(1-m_E;\frac{1}{\xi_E},\frac{1}{\xi_E}),(1-m_{sE};\frac{1}{\xi_{sE}},\frac{1}{\xi_{sE}})\\ -\end{matrix}\middle\vert \begin{matrix}(1,1),(1,1)\\ (1,1),(0,1)\end{matrix}\middle\vert \begin{matrix}(1,1)\\ (m_B,\frac{1}{\xi_B}),(m_{sB},\frac{1}{\xi_{sB}}),(0,1)\end{matrix}\right]$
	$-\frac{\kappa_E}{\lambda_E} H_{2,4}^{4,1}\left[\frac{1}{\lambda_E}\middle\vert \begin{matrix}(1,1),(1,1)\\ (1,1),(m_E-\frac{1}{\xi_E},\frac{1}{\xi_E}),(m_{sE}-\frac{1}{\xi_{sE}},\frac{1}{\xi_{sE}}),(0,1)\end{matrix}\right]$

Taking the case of $\alpha-\mu$ distribution as an example, the lower bound of the SOP is given by

$$\mathscr{P}_{out}^{L}=1-\frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}H_{2,2}^{2,1}\left[\frac{\lambda_B R_s}{\lambda_E}\middle|\begin{matrix}\left(1-\mu_E,\frac{1}{\alpha_E}\right),(1,1)\\(0,1),\left(\mu_B,\frac{1}{\alpha_B}\right)\end{matrix}\right]. \tag{5.23}$$

For the sake of high accuracy, the asymptotic SOP at high $\bar{\gamma}_B$ regime is evaluated at $\tau=0$ and $\tau=-\alpha_B\mu_B$, and is given by Kong *et al.* (2018c)

$$\mathscr{P}_{out}\approx\frac{\Gamma\left(\frac{\alpha_B\mu_B}{\alpha_E}+\mu_E\right)}{\Gamma(1+\mu_B)\Gamma(\mu_E)}\left(\frac{R_s\lambda_B}{\lambda_E}\right)^{\alpha_B\mu_B}. \tag{5.24}$$

5.6.2 Asymptotic PNZ

The asymptotic PNZ at high or low $\bar{\gamma}_B$ regime, is computed by evaluating the residues of analytical PNZ, given in (5.16). According to Rahama *et al.* (2018), Fox's H-function can be further simplified by choosing the dominate term of the Mellin-Barnes type integral. As such, we can evaluate the residue of the PNZ at low $\bar{\gamma}_B$ regime, at the point

$$\tau=\min_{l=1:m_1,i=1:n_0}\left(-\frac{d_l+D_l}{D_l},\frac{a_i+A_i-1}{A_i}\right),g=\operatorname*{argmin}_{l=1:m_1,i=1:n_0}\left(-\frac{d_l+D_l}{D_l},\frac{a_i+A_i-1}{A_i}\right). \tag{5.25a}$$

Assuming the case of a simple pole, the asymptotic PNZ is thereafter given in (5.26).

$$\begin{aligned}\mathscr{P}_{nz}\approx&\frac{\Gamma(-\tau)\prod_{l=1,l\neq g}^{m_1}\Gamma(d_l+D_l+D_l\tau)\prod_{i=1,i\neq g}^{n_0}\Gamma(1-a_i-A_i+A_i\tau)}{\Gamma(1-\tau)\prod_{i=n_0+1}^{p_0}\Gamma(a_i+A_i-A_i\tau)\prod_{l=m_1+1}^{q_1}\Gamma(1-d_l-D_l-D_l\tau)}\\&\frac{\prod_{i=1}^{n_1}\Gamma(1-c_i-C_i-C_i\tau)\prod_{l=1}^{m_0}\Gamma(b_l+B_l-B_l\tau)}{\prod_{i=n_1+1}^{p_1}\Gamma(c_i+C_i+C_i\tau)\prod_{l=m_0+1}^{q_0}\Gamma(1-b_l-B_l+B_l\tau)}\left(\frac{\lambda_B}{\lambda_E}\right)^{s}\frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}.\end{aligned} \tag{5.26}$$

Considering the case of $\alpha-\mu$ as an example, applying the obtained result, the asymptotic PNZ at low $\bar{\gamma}_B$ regime is evaluated at $s=-\alpha_E\mu_E$ and thereafter given by

$$\mathscr{P}_{nz}\approx\frac{\kappa_B\kappa_E}{\lambda_B\lambda_E\mu_E}\Gamma\left(\frac{\alpha_E\mu_E}{\alpha_B}+\mu_B\right)\left(\frac{\lambda_E}{\lambda_B}\right)^{\alpha_E\mu_E}. \tag{5.27}$$

5.6.3 Asymptotic ASC

By applying the expansion rule, in the case of high $\bar{\gamma}_B$, the asymptotic ASC is given by (5.28), which is obtained by individually expanding I_1 and I_2, respectively.

$$\begin{aligned}
I_1\approx&\frac{\kappa_B\kappa_E}{\lambda_B\lambda_E}\left[\ln\left(\frac{1}{\lambda_B}\right)+\sum_{l=1}^{m_0}B_l\Psi_0(b_l+B_l+B_lu)-\sum_{l=m_l+1}^{q_0}B_l\Psi_0(b_l+B_l+B_lu)\right.\\
&\left.-\sum_{i=1}^{p_0}A_i\Psi_0(a_i+A_i+A_iu)\right]\frac{\Gamma(u)\prod\limits_{l=1,l\neq g}^{m_0}\Gamma(b_l+B_l+B_lu)\prod\limits_{i=1,i\neq g}^{n_1}\Gamma(1-c_i-C_i+C_iu)}{\Gamma(1+u)\prod\limits_{l=m_1+1}^{q_0}\Gamma(1-b_l-B_l-B_lu)\prod\limits_{i=n_1+1}^{p_0}\Gamma(a_i+A_i+A_iu)},\\
&\times\frac{\prod\limits_{l=1}^{m_1}\Gamma(d_l+D_l-D_lu)}{\prod\limits_{i=n_2+1}^{p_1}\Gamma(c_i+C_i-C_iu)\prod\limits_{l=m_2+1}^{q_1}\Gamma(1-d_l-D_l-D_lu)}\left(\frac{\lambda_E}{\lambda_B}\right)^s\\
&\text{where } u=\max_{l=1:m_0,i=1:n_1}\left[0,\left(-\frac{b_l+B_l}{B_l}\right)_{l=1:m_0},\left(\frac{c_i+C_i-1}{c_i}\right)_{i=1:n_1}\right],\\
&g=\operatorname*{argmax}_{l=1:m_0,i=1:n_1}\left[0,\left(-\frac{b_l+B_l}{B_l}\right)_{l=1:m_0},\left(\frac{c_i+C_i-1}{c_i}\right)_{i=1:n_1}\right],
\end{aligned} \tag{5.28a}$$

$$I_2 \approx \prod_{l=1,l\neq g}^{m_0} \Gamma(b_l + B_l - B_l u) \left(\frac{\lambda_E}{\lambda_B}\right)^u \frac{\kappa_B \kappa_E}{\lambda_B \lambda_E} \frac{\Gamma(u) \prod_{i=1}^{n_0} \Gamma(1 - a_i - A_i + A_i u)}{\Gamma(1+u) \prod_{i=1}^{n_0+1} \Gamma(a_i + A_i - A_i u) \prod_{l=1}^{m_0+1} \Gamma(1 - b_l - B_l + B_l u)}$$
$$\times H_{q_1+2,p_1+2}^{n_1+1,m_1+2} \left[\lambda_E \left| \begin{matrix} (1,1),(1,1),(1-d_l-D_l,D_l)_{l=1:p_1},(1,1) \\ (0,1),(0,1),(d_l+D_l+D_l s),(1-c_i-C_i,C_i)_{i=1:q_1} \end{matrix} \right. \right],$$
$$\text{where } u = 1 + \min \left(\frac{b_l}{B_l}\right)_{l=1:m_0}, g = \underset{l=1:m_0}{\operatorname{argmin}} \left(\frac{b_l}{B_l}\right). \tag{5.28b}$$

The detailed proof for (5.28) is referenced to Appendix. II.3.

Similarly, taking the case of $\alpha - \mu$ as an example, we get the asymptotic ASC at high $\bar{\gamma}_B$ regime as

$$I_1 \approx \frac{\kappa_B \kappa_E}{\lambda_B \lambda_E} \Gamma(\mu_B) \Gamma(\mu_E) \left[\frac{\Psi_0(\mu_B)}{\alpha_B} - \ln(\lambda_B) \right], \tag{5.29a}$$

$$I_2 \approx \frac{\kappa_B \kappa_E \left(\frac{\lambda_B}{\lambda_E}\right)^{\alpha_B \mu_B}}{\mu_B \lambda_B \lambda_E} H_{2,3}^{3,1} \left[\lambda_E \left| \begin{matrix} (0,1),(1,1) \\ (\mu_E + \frac{\alpha_B \mu_B}{\alpha_E}, \frac{1}{\alpha_E}),(0,1),(0,1) \end{matrix} \right. \right]. \tag{5.29b}$$

5.7 Colluding Eavesdropping Scenario

In this section, we mainly focus on the secrecy issue when multiple eavesdroppers appear and work in a cooperative manner.

5.7.1 System Model

Consider the scenario that L eavesdroppers are in the presence and work cooperatively to wiretap the main link. It is assumed that all L eavesdroppers are single-antenna equipped, and undergoes independent fading conditions. As a result of collusion Cho, S., Chen, G. & Coon, J. P. (2018), the so-called eavesdropper is assumed to either use the MRC or the SC scheme. All the wiretap links and main link undergo independent Fox's H-function fading channels. Consequently, the instantaneous received SNR at the so-called L-colluding eavesdropper with

MRC scheme is given by

$$\gamma_C = \sum_{r=1}^{L} \gamma_{e,r}, \tag{5.30}$$

or with SC scheme

$$\gamma_C = \max\{\gamma_{e,1}, \cdots, \gamma_{e,l}, \cdots, \gamma_{e,L}\}, \tag{5.31}$$

where $\gamma_{e,r}$ is the instantaneous received SNR of each eavesdropper. Clearly, (5.30) corresponds to a maximum ratio combining (MRC) decoding which is the best strategy that the super eavesdropper can use. As we can see from (5.30), γ_C is the sum of L independent Fox's H-function distributed RVs, the PDF and CDF of γ_C are thus respectively given by (Rahama *et al.*, 2018, eqs. (8) and (9))

$$f_C(\gamma) = \frac{\eta_C}{\gamma} H\left[\begin{array}{c|c|c} \begin{matrix}(0,0)\\(0,1)\end{matrix} & - & \\ \begin{matrix}(m_r, n_r+1)\\(p_r+1, q_r)\end{matrix}_{r=1:L} & \begin{matrix}(1;(1)_{r=1:L})\\ \left[\begin{matrix}(1,1),(c_i+C_i,C_i)_{i=1:q_r}\\(d_l+D_l,D_l)_{l=1:p_r}\end{matrix}\right]_{r=1:L}\end{matrix} & (\lambda_r\gamma)_{r=1:L} \end{array}\right], \quad \gamma > 0, \tag{5.32a}$$

$$F_C(\gamma) = \eta_C H\left[\begin{array}{c|c|c} \begin{matrix}(0,0)\\(0,1)\end{matrix} & - & \\ \begin{matrix}(m_r, n_r+1)\\(p_r+1, q_r)\end{matrix}_{r=1:L} & \begin{matrix}(0;(1)_{r=1:L})\\ \left[\begin{matrix}(1,1),(c_i+C_i,C_i)_{i=1:q_r}\\(d_l+D_l,D_l)_{l=1:p_r}\end{matrix}\right]_{r=1:L}\end{matrix} & (\lambda_r\gamma)_{r=1:L} \end{array}\right], \tag{5.32b}$$

where $\eta_C = \prod_{e=1}^{M} \frac{\kappa_{E,e}}{\lambda_{E,e}}$.

Similarly, the PDF and CDF of instantaneous SNR deployed with SC scheme is given by Kong, N. & Milstein, L. B. (1999)

$$f_C(\gamma) = \sum_{\tau=1}^{L} f_{e,\tau}(\gamma) \prod_{l=1, l\neq\tau}^{L} F_{e,l}(\gamma), \tag{5.33a}$$

$$F_C(\gamma) = \prod_{l=1}^{L} F_{e,l}(\gamma), \tag{5.33b}$$

where $f_{e,\tau}(\gamma)$ and $F_{e,l}(\gamma)$ are the corresponding PDF and CDF of the instantaneous received SNR of each eavesdropper, which are given in terms of univariate Fox's H-function.

It is worthy to mention that the multivariate Fox's H-function PDF and CDF of the equivalent super-eavesdropper makes it difficult to seek the exact SOP and ASC for the colluding scenario. Resultantly, we intend to provide the lower bound of the SOP and exact PNZ for this case.

5.7.2 Secrecy Characterization of SOP

Theorem 7. *The SOP over Fox's H-function wiretap fading channels in the presence of L-colluding eavesdroppers with MRC scheme is lower bounded by (5.34),*

$$\mathscr{P}^{L}_{out,MRC} = \frac{\eta_C \kappa_B}{\lambda_B} H \left[\begin{matrix} \begin{pmatrix} n_0+1, m_0 \\ q_0+1, p_0+2 \end{pmatrix} \\ \begin{pmatrix} m_r, n_r+1 \\ p_r+1, q_r \end{pmatrix}_{r=1:L} \end{matrix} \middle| \begin{matrix} (1-b_i-B_i,(B_i)_{r=1:L}),(1,(1)_{r=1:L}) \\ (0,(1)_{r=1:L}),(1-a_i-A_i,(A_i)_{r=1:L}),(1,(1)_{r=1:L}) \\ \begin{bmatrix} (1,1),(c_i+C_i,C_i)_{i=1:q_2} \\ (d_l+D_l,D_l)_{l=1:p_2} \end{bmatrix}_{r=1:L} \end{matrix} \middle| \left(\frac{\lambda_{e,r}}{\lambda_B R_s}\right)_{r=1:L} \right]. \tag{5.34}$$

Proof. Plugging (5.5b) and (5.32a) into

$$\mathscr{P}_{out,MRC} = \int_0^\infty F_B(\gamma_0) f_C(\gamma_C) d\gamma_C,$$

then re-expressing the univariate Fox's H-function and multivariate Fox's H-function in terms of their definition, and performing the interchange of the Mellin-Barnes integrals and the definite integral, with the help of (Gradshteyn & Ryzhik, 2014, eqs.(3.194.3) and (8.384.1)), we arrive at the final expression of $\mathscr{P}_{out,MRC}$ in (5.34). □

Theorem 8. *The SOP over Fox's H-function wiretap fading channels in the presence of L-colluding eavesdroppers with SC scheme is lower bounded by (5.35),*

$$\mathscr{P}^{L}_{out,SC}=\sum_{l=1}^{L}\frac{\eta_C\kappa_B}{\lambda_B}H\left[\begin{array}{c|c|c}\begin{pmatrix}n_l,m_l\\q_l,p_l\end{pmatrix}&(1-d_i+D_i,(D_i)_{r=1:L})&\\ \begin{pmatrix}m_0,n_0+1\\p_0+1,q_0+1\end{pmatrix}&(1-c_i+C_i,(C_i)_{r=1:L})&\\ \begin{pmatrix}m_r,n_r+1\\p_r+1,q_r\end{pmatrix}_{r=1:l-1}&(1,1),(a_i+A_i,A_i)_{i=1:p_0}&\\ \begin{pmatrix}m_{r+1},n_{r+1}+1\\p_{r+1}+1,q_{r+1}+1\end{pmatrix}_{r=l+1:L}&(b_l+B_l,B_l)_{l=1:q_0}&\\ &\begin{bmatrix}(1,1),(c_i+C_i,C_i)_{i=1:p_r}\\(d_l+D_l,D_l)_{l=1:q_r},(0,1)\end{bmatrix}_{r=1:l-1}&\left(\frac{\lambda_{e,r}}{\lambda_{e,l}}\right)_{r=1:l-1}\\ &\begin{bmatrix}(1,1),(c_i+C_i,C_i)_{i=1:p_r}\\(d_l+D_l,D_l)_{l=1:q_r},(0,1)\end{bmatrix}_{r=l+1,L}&\left(\frac{\lambda_{e,r}}{\lambda_{e,l}}\right)_{r=l+1:L}\end{array}\right]^{\frac{\lambda_B}{\lambda_{e,l}}}. \tag{5.35}$$

Proof. Accordingly, by doing some simple substitutions, $\mathscr{P}^{L}_{out,SC}$ can be rewritten as

$$\mathscr{P}^{L}_{out,SC}=\sum_{\tau=1}^{L}\int_0^{\infty}F_B(R_s\gamma)f_{e,\tau}(\gamma)\prod_{l=1,l\neq\tau}^{L}F_{e,l}(\gamma)d\gamma, \tag{5.36}$$

then using the Mellin transform of multiple univariate Fox's H-function, the proof is achieved.

□

5.7.3 Secrecy Characterization of PNZ

Theorem 9. *The PNZ over Fox's H-function wiretap fading channels in the presence of L-colluding eavesdroppers with MRC scheme is given by (5.37),*

$$\mathscr{P}_{nz,MRC}=\frac{\eta_C\kappa_B}{\lambda_B}H\left[\begin{array}{c|c|c}\begin{pmatrix}n_0,m_0\\q_0,p_0+1\end{pmatrix}&(1-b_i-B_i;(B_i)_{r=1:L})_{i=1:q_0}&\\ \begin{pmatrix}m_r,n_r+1\\p_r+1,q_r\end{pmatrix}_{r=1:L}&(1-a_i-A_i;(A_i)_{r=1:L})_{i=1:p_0},(0;(1)_{r=1:L})&\left(\frac{\lambda_{e,r}}{\lambda_B}\right)_{r=1:L}\\ &\begin{bmatrix}(1,1),(c_i+C_i,C_i)_{i=1:q_r}\\(d_l+D_l,D_l)_{l=1:p_r}\end{bmatrix}_{r=1:L}&\end{array}\right], \tag{5.37}$$

Proof. Substituting (5.5a) and (5.32b) into (5.9), then re-expressing the multivariate Fox's H-function in terms of its definition and interchanging the order of two integrals, we obtain (5.37). □

Theorem 10. *The PNZ over Fox's H-function wiretap fading channels in the presence of L-colluding eavesdroppers with SC scheme is given by (5.38),*

$$\mathscr{P}_{nz,SC} = \frac{\eta_C \kappa_B}{\lambda_B} H \left[\begin{array}{c|c|c} \begin{matrix} (n_0, m_0) \\ (q_0, p_0) \end{matrix} & \begin{matrix} (1-b_i-B_i;(B_i)_{r=1:L})_{i=1:q_0} \\ (1-a_i-A_i;(A_i)_{r=1:L})_{i=1:p_0} \end{matrix} & \left(\frac{\lambda_{e,r}}{\lambda_B}\right)_{r=1:L} \\ \left(\begin{matrix} m_r, n_r+1 \\ p_r+1, q_r+1 \end{matrix}\right)_{r=1:L} & \left[\begin{matrix} (1,1),(c_i+C_i,C_i)_{i=1:q_r} \\ (d_l+D_l,D_l)_{l=1:p_r},(0,1) \end{matrix}\right]_{r=1:L} & \end{array} \right]. \tag{5.38}$$

Proof. Substituting (5.5a) and (5.33b) into

$$\mathscr{P}_{NZ,SC} = \int_0^\infty f_B(\gamma_B) F_{C,SC}(\gamma_B) d\gamma_B = \int_0^\infty f_B(\gamma_B) \prod_{l=1}^{L} F_{e,l}(\gamma_B) d\gamma_B, \tag{5.39}$$

then following the same methodology used in Theorem 8, the proof is obtained. □

5.8 Numerical Results and Discussions

In this section, Monte-Carlo simulations are used to validate the analytical derivations obtained in Sections 5.5 and 5.7, particularly, over one special case of Fox's H-function wiretap fading channel, i.e., $\alpha-\mu$ wiretap fading channels[2]. It is noted that bullets represent the simulation results whereas solid lines are used to show the analytical expressions.

[2] It is worthy to mention that (i) the α-μ fading channel is implemented by using the WAFO toolboxBrodtkorb *et al.* (2000); (ii) the numerical evaluation of univariate and bivariate Fox's H-function for MATLAB implementations are based on the method proposed in (Peppas *et al.*, 2012, Table. II) and (Peppas, 2012, Appendix. A), respectively.

5.8.1 Non-colluding Scenario

In order to validate the analytical accuracy of our derivations, Monte-Carlo simulation outcomes together with analytical results are presented in Figs. 5.1-5.3, with regard to the aforementioned three secrecy performance metrics over $\alpha-\mu$ fading channels. Apparently, these figures show that our mathematical representations are in perfect agreements with the simulation results.

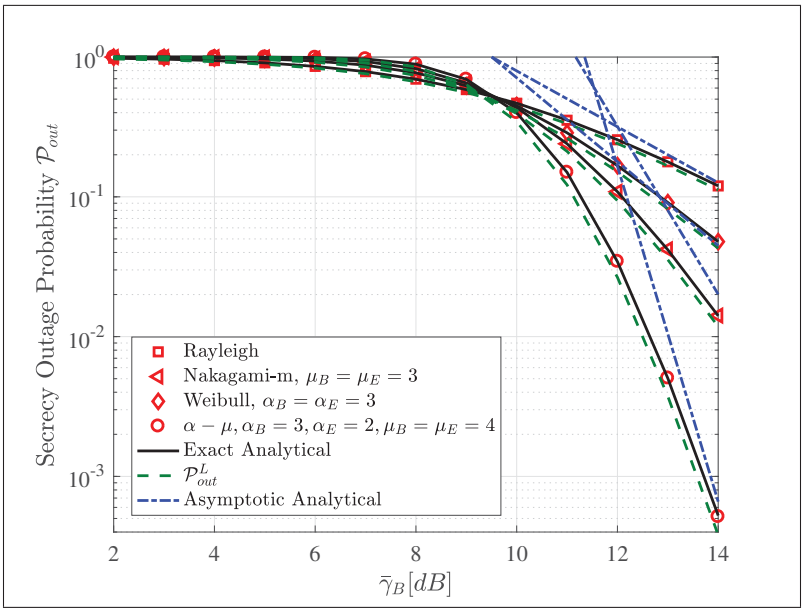


Figure 5.1 $\mathscr{P}_{out}$ versus the average $\bar{\gamma}_B$ over Rayleigh, Nakagami-m, Weibull and $\alpha-\mu$ fading channels when $\bar{\gamma}_E=0$ dB and $R_t=0.5$, respectively.

In Fig. 5.1, the SOP against $\bar{\gamma}_B$ is plotted for several fading scenarios, such as Rayleigh, Weibull, Nakagami-m, and $\alpha-\mu$. As observed from the figure, specifically, the Nakagami-m ($\alpha=2$, $\mu=m$) against Rayleigh ($\alpha=2$, $\mu=1$), and Rayleigh against Weibull (α is the fading parameter, $\mu=1$), one can conclude that larger α and μ values result in lower SOP. This is mainly because lower α and μ values represent serious non-linearity and sparse clustering, i.e., worse channel conditions Lei *et al.* (2017a). This phenomenon also remains true for the PNZ, as shown in Fig. 5.2. In addition, the lower bound of SOP and the asymptotic SOP are

also plotted. It is observed that the lower bound of the SOP, i.e., $\mathscr{P}_{out}^{L}$ offers a better SOP performance trend prediction, on the other hand, the asymptotic SOP gradually approximates the exact SOP with higher accuracy as $\bar{\gamma}_B$ increases.

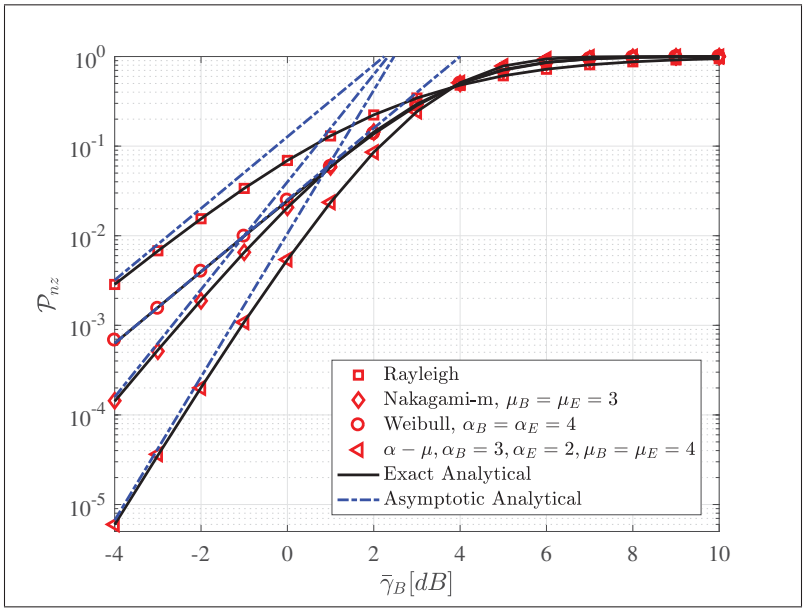


Figure 5.2 $\mathscr{P}_{nz}$ versus the average $\bar{\gamma}_B$ for selected fading parameters when $\bar{\gamma}_E$ = 4 dB.

As depicted in Fig. 5.2, both the exact and asymptotic behavior of $\mathscr{P}_{nz}$ are plotted against $\bar{\gamma}_B$ for Rayleigh, Weibull, Nakagami-m, and $\alpha - \mu$. Compared with the exact result, one can conclude that our asymptotic PNZ behaves well at low $\bar{\gamma}_B$ regime.

The ASC against the ratio of $\bar{\gamma}_B$ and $\bar{\gamma}_E$ is presented in Fig. 5.3, and as expected, there is a perfect match between our analytical and simulated results. Also, one can obtain two insights from this graph: on one hand, lower α values lead to higher ASC, no matter whoever experiences severe fading.

The insight obtained from this figure just vividly demonstrates how information-theoretic security exploits the fading property of wireless transmission medium to ensure secure transmission.

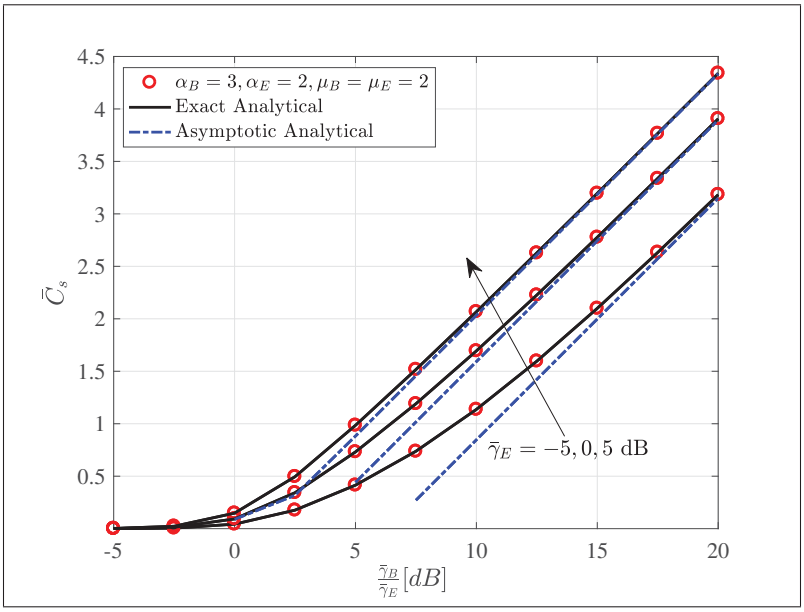


Figure 5.3 $\bar{C}_s$ versus $\frac{\bar{\gamma}_B}{\bar{\gamma}_E}$ over $\alpha - \mu$ wiretap fading channels.

On the other hand, a potential malicious eavesdropper can also benefit from poor channel conditions, since worse fading channels reversely enable them to better access and wiretap the main channel to a certain extent. Finally, to obtain a fair comparison, the asymptotic ASC is also depicted in Fig. 5.3. Again, it can be seen that the asymptotic ASC presents a highly accurate approximation to the exact ASC, especially at high $\bar{\gamma}_B$ regime.

5.8.2 Colluding Scenario

In this subsection, both the lower bound of SOP and PNZ are presented over $\alpha - \mu$, F-S $\mathscr{F}$, and EGK fading channels, respectively. For the simplicity of notations, it is assummed that all eavesdroppers undergo similar fading condition, i.e., similar fading parameters. It is noted that the implementation of multivariate Fox's H-function is available in Python (Alhennawi *et al.*, 2016, Appendix A) and MATLAB Chergui, H., Benjillali, M. & Alouini, M.-S. (2018).

Figs. 5.4 demonstrates the analytical $\mathscr{P}^L_{MRC,out}$ and $\mathscr{P}^L_{SC,out}$ together with simulated SOP over $\alpha - \mu$ fading channels. One can perceive that our derived lower bound of SOP can closely

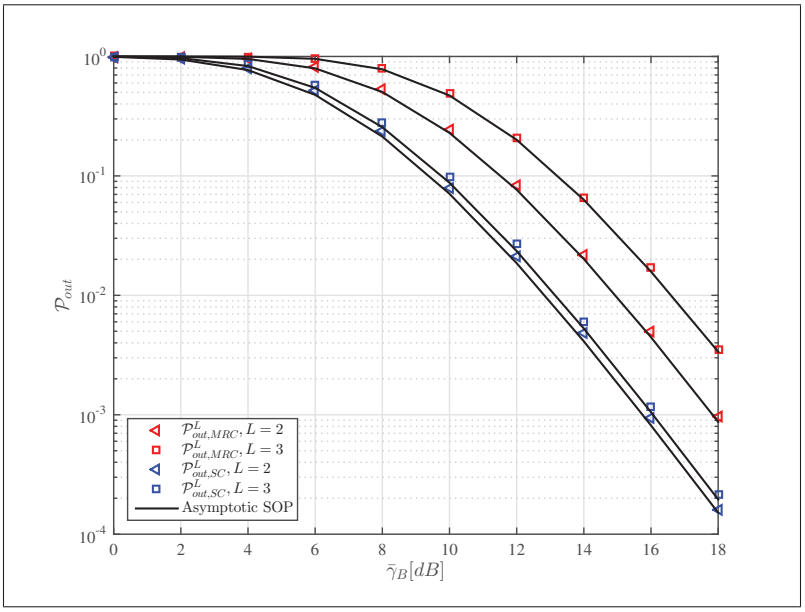


Figure 5.4 The lower bound of SOP, i.e., $\mathscr{P}^L_{out}$ over $\alpha-\mu$ fading channels when $\alpha_B=2, \alpha_E=4, \mu_B=\mu_E=3$

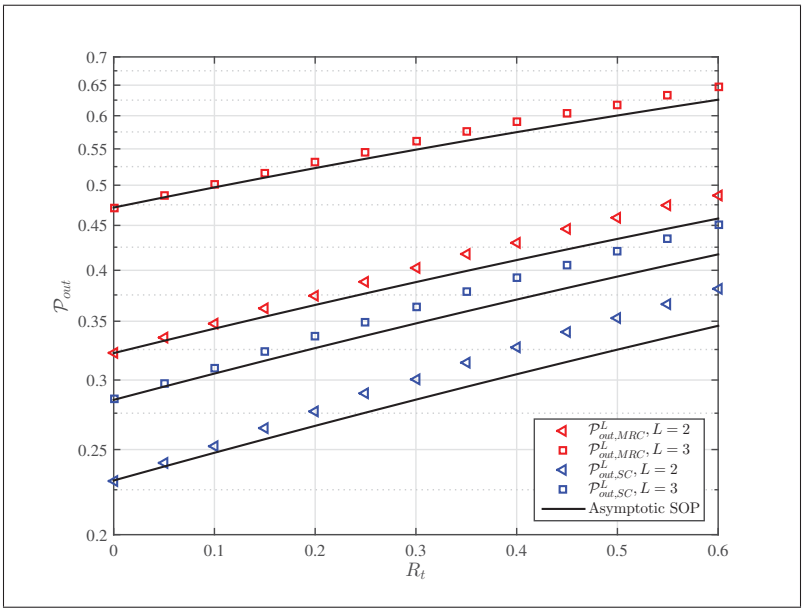


Figure 5.5 The lower bound of SOP, i.e., $\mathscr{P}^L_{out}$ over EGK fading channels when $m_B=m_E=2, m_{sB}=m_{sE}=4, \xi_B=\xi_{sB}=\xi_E=\xi_{sE}=1$.

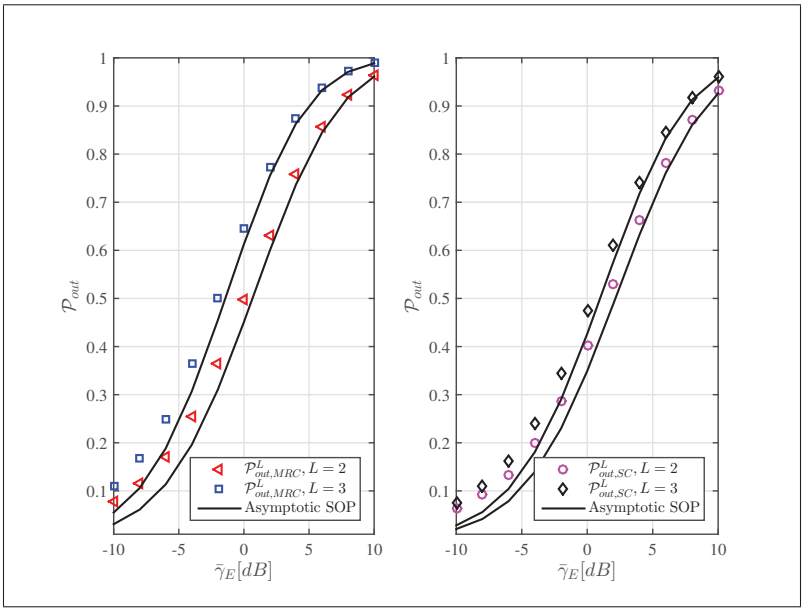


Figure 5.6 The lower bound of SOP, i.e., $\mathscr{P}^L_{out}$ over F-S $\mathscr{F}$ fading channels when $\mathscr{F}$, $m_B = m_E = 2, m_{B,s} = m_{E,s} = 3$.

approximate the exact SOP. As the number of cooperative eavesdroppers increases, the gap between the lower bound of SOP and exact SOP gradually becomes smaller.

On the other hand, the increase of the number of L contributes largely to the $\mathscr{P}^L_{out,MRC}$ when MRC scheme is employed, compared to the $\mathscr{P}_{out,SC}$ case.

Apart from Fig. 5.4, we also compared the simulated and analytical SOPs for the following two scenarios: (i) changing γ_E while fixing R_t, as shown in Fig.5.5; and (ii) changing R_t while keeping γ_E constant, as depicted in Fig. 5.6. Apparently, one can obtain the following two observations. On one hand, Fig. 5.5 shows that the lower bound of the SOP is becoming increasingly tight with the decrease of lower R_t. Different from 5.5, Fig.5.6 portrays that higher $\bar{\gamma}_E$ makes the lower bound of SOP sufficiently approximates the exact SOP. Those two observations can be mathematically explained from the definition of the lower bound of SOP, i.e., $\mathscr{P}(\gamma_B < (R_s\gamma_C + \mathscr{W})) \approx \mathscr{P}(\gamma_B < (R_s\gamma_C))$. This condition can be met when R_t goes to 0 ($\mathscr{W} = 2^{R_t} - 1$), or $\gamma_C \gg \mathscr{W}$.

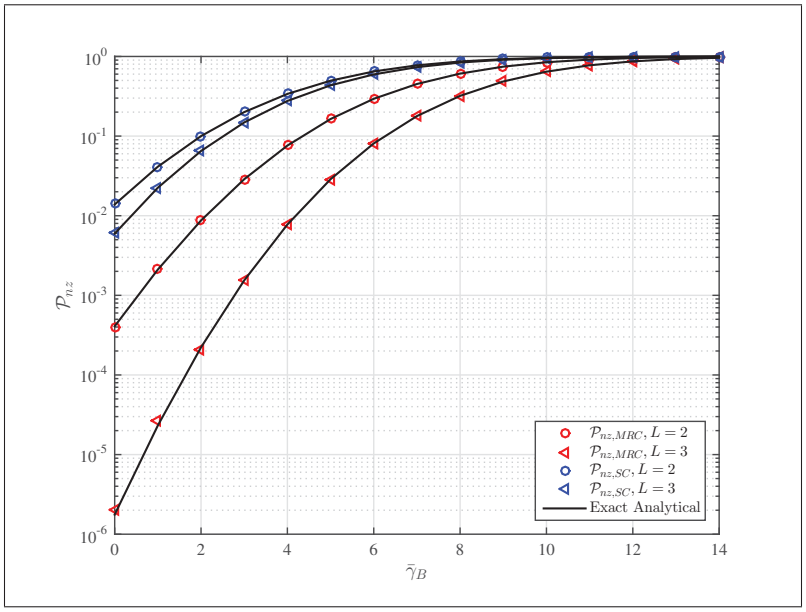


Figure 5.7 $\mathscr{P}_{nz,MRC}$, $\mathscr{P}_{nz,SC}$ versus $\bar{\gamma}_B$ over $\alpha-\mu$ wiretap fading channels when $\alpha_B = 2, \alpha_E = 4, \mu_B = \mu_E = 3$.

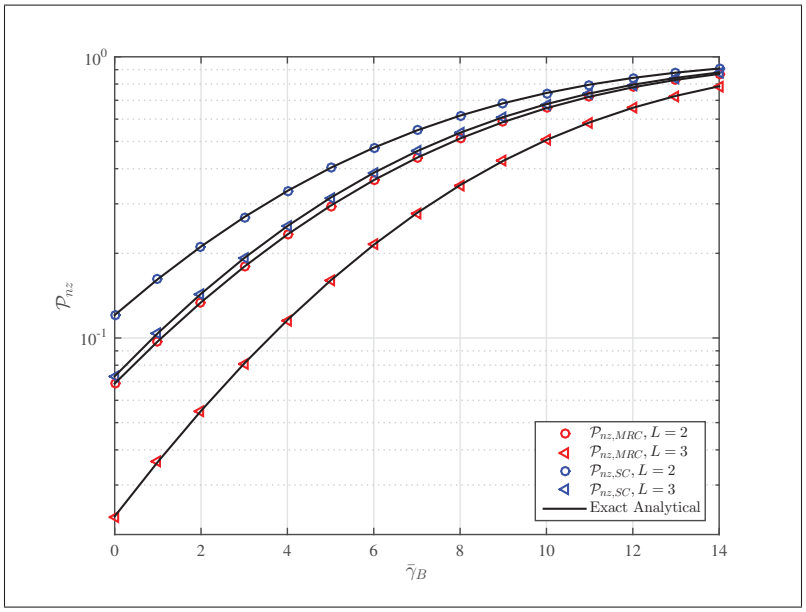


Figure 5.8 $\mathscr{P}_{nz,MRC}$, $\mathscr{P}_{nz,SC}$ versus $\bar{\gamma}_B$ over F-S $\mathscr{F}$ wiretap fading channels when $m_B = m_E = 2, m_{s,B} = m_{s,E} = 3$.

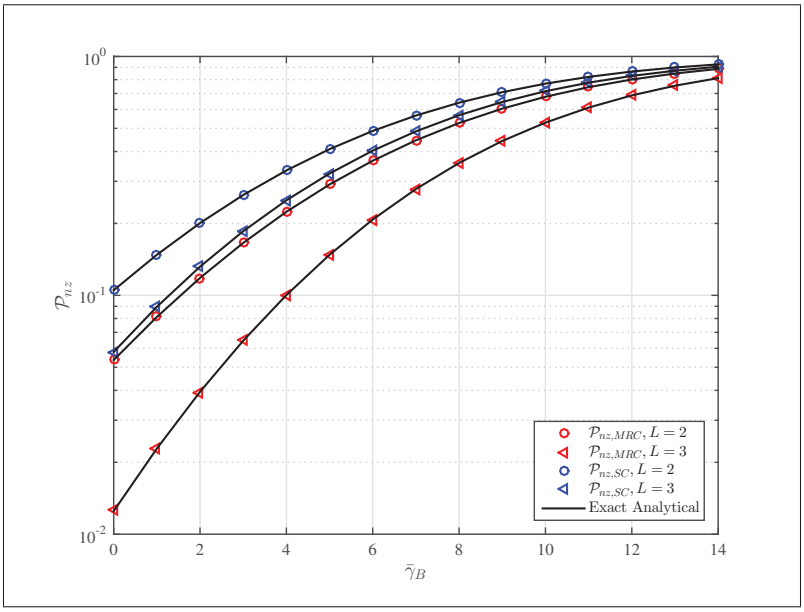


Figure 5.9 $\mathscr{P}_{nz,MRC}$, $\mathscr{P}_{nz,SC}$ versus $\bar{\gamma}_B$ over EGK wiretap fading channels when $m_B = m_E = 2, m_{sB} = m_{sE} = 4$, $\xi_B = \xi_{sB} = \xi_E = \xi_{sE} = 1$.

Likewise, in Figs. 5.7-5.9, the PNZ given in (5.37) and (5.38) are plotted and compared with Monte-Carlo simulation. The validity of our presented PNZ expressions are examined over the $\alpha - \mu$, F-S $\mathscr{F}$, and EGK fading channels, respectively.

Each figure witnesses perfect agreements between the exact analysis and simulated results. Besides, it is clear that the influences of L on $\mathscr{P}_{nz,MRC}$ is larger than that on $\mathscr{P}_{nz,SC}$. This is obviously due to the MRC and SC schemes.

5.9 Conclusion

Since Fox's H-function fading channel can subsume most of the fading models, this paper comprehensively investigated the PLS over Fox's H-function wiretap fading channels, with consideration of the non-colluding and colluding eavesdropping scenarios. For the former non-colluding case, secrecy metrics, including the SOP, PNZ, and ASC, are derived with closed-form expressions in a general and unified manner. Those expressions are given in terms of

the univariate or bivariate Fox's H-function. In addition, those closed-form expressions were further simplified to acquire the asymptotic behavior of the secrecy metrics. The asymptotic ones were much simpler and highly accurate for practical usage. In the presence of colluding eavesdroppers, a super eavesdropper employing by MRC or SC schemes were formulated, and subsequently the lower bound of SOP and the exact PNZ were provided in terms of multivariate Fox's H-function. Both scenarios are further demonstrated by Monte-Carlo simulations.

In addition, for the sake of providing more insights on some well-known fading models, several special cases of Fox's H-function distribution were particularly explored, including $\alpha - \mu$, F-S $\mathscr{F}$, and EGK. Those examples were further elaborated with the general form, and their accuracy was also compared with Monte-Carlo simulation results. As observed and discussed, the advantages of those general mathematical representations are listed as follows: (i) they are consistent with the existing works; (ii) they provide a unified generic approach to other fading models which can be expanded in terms of Fox's H-function fading distribution; and (iii) they provide a promising secrecy performance analysis framework when colluding eavesdroppers are undergoing different independent fading conditions.

CHAPTER 6

SECRECY CHARACTERISTICS WITH ASSISTANCE OF MIXTURE GAMMA DISTRIBUTION

Long Kong and Georges Kaddoum

Département de Génie électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3.

Paper published in IEEE Wireless Communications Letters, March 2019.

6.1 Abstract

Considering the fact that the mixture gamma (MG) distribution is a general model that can be used to elaborate most well-known distributions, including small-scale, large-scale, and composite fadings, this letter studies the security issue when the received signal-to-noise ratios (SNRs) follow MG distributions. Closed-form expressions for secrecy metrics including the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), and the average secrecy capacity (ASC), are derived. Monte-Carlo simulations are presented to corroborate the accuracy of our derived results. Our derived secrecy metrics provide a general and unified analysis framework for the quick evaluation of the secrecy issue over wireless channels, even when the main channel and wiretap channel are subject to different wireless channels.

Keywords: Physical layer security (PLS), Mixture Gamma (MG) distribution, Meijer's *G*-function

6.2 Introduction

Physical layer security (PLS) is viewed as a promising fundamental security mechnism since it is theoretically supported by two fundamental works, i.e., Shannon's information theoretic formulation and Wyner's wiretap model. Numerous works have demonstrated that the random-

ness of the wireless medium is essentially beneficial and can be reversely used to boost secrecy concerns Bloch *et al.* (2008).

Therefore, physical layer security has drawn significant research interests. In particularly, secrecy metrics have been essentially analyzed over four kinds of fading channels: (i) small-scale fading, e.g., Nakagami Liu, W., Vuppala, S., Abreu, G. & Ratnarajah, T. (2014), Nakagami-*n* (Rician) Liu (2013a), Nakagami-*q* (Hoyt) Romero-Jerez, J. M. & Lopez-Martinez, F. J. (2017), $\alpha-\mu$Kong *et al.* (2016b,1); Lei *et al.* (2017a), $\kappa-\mu$ Iwata *et al.* (2017), $\alpha-\eta-\kappa-\mu$ Mathur *et al.* (2018) (ii) large-scale fading, e.g., lognormal Pan *et al.* (2016), (iii) cascaded fading, e.g., cascaded $\alpha-\mu$ Kong *et al.* (2018a); (iv) composite fading, e.g., generalized-$\mathcal{K}$ ($\mathcal{K}_G$) Lei *et al.* (2016c), Fisher-Snedecor $\mathcal{F}$ Kong & Kaddoum (2018). More recently, the mixture gamma (MG) distribution was proposed by Atapattu *et al.* in Atapattu, S., Tellambura, C. & Jiang, H. (2011) to model the signal-to-noise ratio (SNR) of wireless channels. This distribution can highly accurately characterize the SNRs of composite fading channels Al-Hmood, H. & Al-Raweshidy, H. S. (2017); Atapattu *et al.* (2011), e.g., $\kappa-\mu$/gamma, $\eta-\mu$/gamma, $\alpha-\mu$/gamma, and $\mathcal{K}_G$, in addition to it being a versatile approximation for any fading SNR Al-Hmood & Al-Raweshidy (2017), e.g., Rayleigh, Nakagami-*q* (Hoyt), Nakagami-*n* (Rician), $\alpha-\mu$, $\eta-\mu$, $\kappa-\mu$. Comprehensively speaking, the MG distribution provides a general approach to model the received SNRs of most fading channels.

Besides the work laid by Lei *et al.* in Lei *et al.* (2016c), they analyzed the secrecy performance over $\mathcal{K}_G$ fading channels by modeling the instantaneous received SNRs at the legitimate and illegitimate users as MG distributed random variables (RVs), where the cumulative distribution functions (CDFs) are characterized with the lower incomplete gamma function $\Upsilon(m,x)$. To the best of the authors' knowledge, no work investigating the physical layer security by modeling the instantaneous received SNRs of wireless channels as MG distributed RVs has been reported.

Although the contribution in Lei *et al.* (2016c) is seemingly fascinating, its constraint by limiting *m* as an integer indeed makes it lack generality. Therefore, in this letter we investigate three secrecy metrics, including the secrecy outage probability (SOP), the probability of non-zero se-

crecy capacity (PNZ), and average secrecy capacity (ASC), over generalized fading conditions by modeling the received SNRs with the MG distribution.

6.3 System model

Consider the Alice-Bob-Eve classic wiretap model, it is assumed that the instantaneous received SNRs $\gamma_i, i \in \{B,E\}$ at Bob and Eve are MG distributed RVs, with probability density functions (PDFs) and CDFs respectively given by Atapattu *et al.* (2011):

$$f_i(\gamma) = \sum_{l=1}^{L_i} \alpha_{i,l}\gamma^{\beta_{i,l}-1}\exp(-\zeta_{i,l}\gamma) \overset{(a)}{=} \sum_{l=1}^{L_i} \alpha_{i,l}\gamma^{\beta_{i,l}-1} H_{0,1}^{1,0}\left[\zeta_{i,l}\gamma \middle| \begin{matrix} - \\ (0,1) \end{matrix}\right], \quad \gamma \geq 0, \tag{6.1a}$$

$$F_i(\gamma) = \sum_{l=1}^{L_i} \alpha_{i,l}\zeta_{i,l}^{-\beta_{i,l}}\Upsilon(\beta_{i,l},\zeta_{i,l}\gamma) \overset{(b)}{=} \sum_{l=1}^{L_i} \alpha_{i,l}\zeta_{i,l}^{-\beta_{i,l}} H_{1,2}^{1,1}\left[\zeta_{i,l}\gamma \middle| \begin{matrix} (1,1) \\ (\beta_{i,l},1),(0,1) \end{matrix}\right], \tag{6.1b}$$

here L_i is the number of terms, and $\alpha_{i,l}, \beta_{i,l}, \zeta_{i,l}$ are the parameters of the ith gamma component. $H_{p,q}^{m,n}[.]$ is the univariate Fox's H-function. Steps (a) and (b) are developed by re-expressing $\exp(\cdot)$ and $\Upsilon(\cdot,\cdot)$ in terms of the unviariate Fox's H-function (Prudnikov *et al.*, 1990, eqs. (8.4.3.1) and (8.4.16.1)), for the sake of assisting the following secrecy metrics derivations.

Assuming the availability of perfect channel state information (CSI) at all terminals and unit distance between both Alice and Bob, and Alice and Eve. According to Bloch *et al.* (2008), the instantaneous secrecy capacity for one realization of (γ_B, γ_E) pair over quasi-static wiretap fading channels is given by

$$C_s(\gamma_B,\gamma_E) = \left[\log_2\left(\frac{1+\gamma_B}{1+\gamma_E}\right)\right]^+, \tag{6.2}$$

where $[x]^+ \triangleq \max(x,0)$.

6.4 Secrecy Characterization

6.4.1 SOP Characterization

The SOP is commonly seen as a crucial secrecy indicator, and widely used when analyzing PLS over fading channels.

Theorem 11. *The SOP is either given by (6.3a) in terms of the bivariate Meijer's G-function (Gradshteyn & Ryzhik, 2014, eq. (9.301)), i.e,* $G_{p,q}^{m,n}[.]$[1]*,*

$$\begin{aligned}\mathscr{P}_{out,1} = &\sum_{k=1}^{L_E}\sum_{l=1}^{L_B}\alpha_{B,l}\alpha_{E,k}\frac{\mathscr{W}\zeta_{E,k}^{1-\beta_{E,k}}}{R_s\zeta_{B,l}^{\beta_{B,l}}}\\ &\times G_{1,0:2,2:1,1}^{0,1:1,1:1,1}\left[\frac{1}{\zeta_{B,l}\mathscr{W}},\frac{R_s}{\zeta_{E,k}\mathscr{W}}\middle|\begin{matrix}(2,1,1)\\ -\end{matrix}\middle|\begin{matrix}(1-\beta_{B,l},1)\\ (0,1)\end{matrix}\middle|\begin{matrix}2-\beta_{E,k}\\ 1\end{matrix}\right],\end{aligned} \tag{6.3a}$$

or given by (6.3b) in terms of the univariate Meijer's G-function Ansari et al. *(2011), i.e.,* $G_{p,q:p_1,q_1:p_2,q_2}^{0,n:m_1.n_1:m_2,n_2}[.]$*,*

$$\mathscr{P}_{out,2} = \sum_{k=1}^{L_E}\sum_{l=1}^{L_B}\frac{\alpha_{B,l}\alpha_{E,k}}{\zeta_{B,l}^{\beta_{B,l}}\zeta_{E,k}^{\beta_{E,k}}}\sum_{n=1}^{\infty}\frac{(-\zeta_{B,l}\mathscr{W})^n}{n!}G_{3,3}^{2,2}\left[\frac{\zeta_{E,k}}{\zeta_{B,l}R_s}\middle|\begin{matrix}(1,1+n-\beta_{B,l},1+n)\\ (\beta_{E,k},n,1+n)\end{matrix}\right]. \tag{6.3b}$$

Proof. For a given target secrecy rate R_t, the SOP is mathematically defined as $\mathscr{P}_{out} = Pr(C_s \leq R_t)$ (Bloch *et al.*, 2008, eq. (9))Kong *et al.* (2018c), and further developed as follows

$$\mathscr{P}_{out} = \int_0^{\infty} F_B(\gamma_0) f_E(\gamma) d\gamma = \sum_{k=1}^{L_E}\sum_{l=1}^{L_B}\int_0^{\infty}\frac{\exp(-\zeta_{E,k}\gamma)\Upsilon(\beta_{B,l},\zeta_{B,l}\gamma_0)}{\left(\alpha_{B,l}\alpha_{E,k}\zeta_{B,l}^{\beta_{B,l}}\right)^{-1}\gamma^{1-\beta_{E,k}}}d\gamma, \tag{6.4}$$

where $\gamma_0 = R_s\gamma + \mathscr{W}, R_s = 2^{R_t}, \mathscr{W} = 2^{R_t} - 1$. Subsequently, plugging (6.1a) and (6.1b) into (6.4), and using (Kong *et al.*, 2018c, eqs. (6-9)), the proof of $\mathscr{P}_{out,1}$ is easily obtained.

[1] It is noted that the bivariate Meijer's *G*-function is computable and programmable in the open literature Ansari, I. S., Al-Ahmadi, S., Yilmaz, F., Alouini, M. & Yanikomeroglu, H. (2011); Chergui *et al.* (2016); Lei *et al.* (2017a); Peppas *et al.* (2012), whereas the univariate Meijer's *G*-function is already available in mathematical software packages, like Mathematica, Maple, MATLAB.

The proof for $\mathscr{P}_{out,2}$ is obtained by applying the Mellin transform of the product of two Meijer's G-functions[2] (Prudnikov *et al.*, 1990, eq. (2.24.1.3)). □

In addition, the lower bound of the SOP $\mathscr{P}_{out}^{L}$ is usually considered when two events happen, i.e., (i) when $R_t \to 0$, which means that Alice adopts no transmission rate, i.e., R_t; (ii) when both γ_B and γ_E operate at high SNR regimes, physically speaking, it is interpreted as the scenario that both Bob and Eve are super close to Alice. As such, $\mathscr{P}_{out}^{L}$ is developed as

$$\mathscr{P}_{out}^{L} = \int_0^{\infty} F_B(R_s\gamma) f_E(\gamma) d\gamma, \tag{6.5}$$

Next, substituting (6.1a) and (6.1b) into (6.5), and using (Prudnikov *et al.*, 1990, eq. (6.455.2)), the lower bound of the SOP is eventually derived as

$$\mathscr{P}_{out}^{L} = \sum_{k=1}^{L_E}\sum_{l=1}^{L_B} \frac{\alpha_{B,l}\alpha_{E,k} R_s^{\beta_{B,l}} \Gamma(\beta_{B,l}+\beta_{E,k})}{\beta_{B,l}\zeta_{E,k}^{\beta_{B,l}+\beta_{E,k}}} {}_2F_1\left(\beta_{B,l}, \beta_{E,k}+\beta_{B,l}; \beta_{B,l}+1; -\frac{\zeta_{B,l}R_s}{\zeta_{E,k}}\right). \tag{6.6}$$

where ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ Gauss Hypergeometric function (Gradshteyn & Ryzhik, 2014, eq. (9.14)).

6.4.2 PNZ Characterization

The PNZ is regarded as another important secrecy metric to measure the existence of the positive secrecy capacity with a probability $\mathscr{P}_{nz}$.

Theorem 12. *The PNZ is given by (6.7)*

$$\mathscr{P}_{nz} = \sum_{k=1}^{L_E}\sum_{l=1}^{L_B} \frac{\alpha_{B,l}\alpha_{E,k} \Gamma(\beta_{E,k}+\beta_{B,l})}{\beta_{E,k}\zeta_{B,l}^{\beta_{B,l}+\beta_{E,k}}} {}_2F_1\left(\beta_{E,k}, \beta_{E,k}+\beta_{B,l}; \beta_{E,k}+1; -\frac{\zeta_{E,k}}{\zeta_{B,l}}\right). \tag{6.7}$$

Proof. Revisiting the definition of $\mathscr{P}_{nz}$, i.e., $\mathscr{P}_{nz} = \int_0^{\infty} F_E(\gamma) f_B(\gamma) d\gamma$, the proof is accomplished by using (Prudnikov *et al.*, 1990, eq. (6.455.2)). □

[2] It is noted that Meijer's G-function is a special case of Fox's H-function (Prudnikov *et al.*, 1990, eq. (8.3.2.21)), i.e., $H_{p,q}^{m,n}\left[x \middle| \begin{matrix}(a_i,\alpha_i)_{i=1:p}\\(c_k,\delta_k)_{k=1:q}\end{matrix}\right] = G_{p,q}^{m,n}\left[x \middle| \begin{matrix}a_i\\c_k\end{matrix}\right]$, when $\alpha_i = \delta_k = 1$.

6.4.3 ASC Characterization

The ASC is a secrecy metric that evaluates how much achievable secrecy rate can be guaranteed for the whole system.

Theorem 13. *The ASC is given by (6.8)*

$$\begin{aligned}\bar{C}_s = &\underbrace{\sum_{k=1}^{L_E}\sum_{l=1}^{L_B}\frac{\alpha_{B,l}\alpha_{E,k}}{\ln(2)\zeta_{B,l}^{\beta_{B,l}}\zeta_{E,k}^{\beta_{E,k}}}G_{1,0:2,2:1,2}^{0,1:1,2:1,1}\left[\frac{1}{\zeta_{B,l}},\frac{\zeta_{E,k}}{\zeta_{B,l}}\middle|\begin{matrix}(1-\beta_{B,l})\\ -\end{matrix}\middle|\begin{matrix}(1,1)\\ (1,0)\end{matrix}\middle|\begin{matrix}(1)\\ (\beta_{E,k},0)\end{matrix}\right]}_{\mathscr{I}_1}\\ &+\underbrace{\sum_{k=1}^{L_E}\sum_{l=1}^{L_B}\frac{\alpha_{B,l}\alpha_{E,k}}{\ln(2)\zeta_{B,l}^{\beta_{B,l}}\zeta_{E,k}^{\beta_{E,k}}}G_{1,0:2,2:1,2}^{0,1:1,2:1,1}\left[\frac{1}{\zeta_{E,k}},\frac{\zeta_{B,l}}{\zeta_{E,k}}\middle|\begin{matrix}(1-\beta_{E,k})\\ -\end{matrix}\middle|\begin{matrix}(1,1)\\ (1,0)\end{matrix}\middle|\begin{matrix}(1)\\ (\beta_{B,l},0)\end{matrix}\right]}_{\mathscr{I}_2}\\ &-\underbrace{\sum_{k=1}^{L_E}\frac{\alpha_{E,k}}{\ln(2)\zeta_{E,k}^{\beta_{E,k}}}G_{3,2}^{1,3}\left[\frac{1}{\zeta_{E,k}}\middle|\begin{matrix}(1,1,1-\beta_{E,k})\\ (1,0)\end{matrix}\right]}_{\mathscr{I}_3}.\end{aligned} \tag{6.8}$$

Proof. By averaging (6.2) over γ_B and γ_E, the ASC is mathematically expressed as (Lei *et al.*, 2016c, eq.(6)), $\bar{C}_s = \mathscr{I}_1 + \mathscr{I}_2 - \mathscr{I}_3$, where $\mathscr{I}_1 = \int_0^\infty \log_2(1+\gamma_B) f_B(\gamma_B) F_E(\gamma_B) d\gamma_B$, $\mathscr{I}_2 = \int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) F_B(\gamma_E) d\gamma_E$, $\mathscr{I}_3 = \int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) d\gamma_E$.

Next, re-expressing $\log(1+x) = \frac{1}{\ln(2)} H_{2,2}^{1,2}\left[x\middle|\begin{matrix}(1,1),(1,1)\\ (1,1),(0,1)\end{matrix}\right]$ (Prudnikov *et al.*, 1990, eq. (8.4.6.5)), and then directly using the Mellin transform of the product of three Fox's H-functions (Mittal, P. & Gupta, K., 1972, eq. (2.3)), the proofs of $\mathscr{I}_1$ and $\mathscr{I}_2$ are obtained Kong & Kaddoum (2018), whereas the proof for $\mathscr{I}_3$ is achieved by applying the Mellin transform of the product of two Fox's H-functions (Prudnikov *et al.*, 1990, eq.(2.25.1.1)) and using (Prudnikov *et al.*, 1990, eq.(8.3.2.21)). □

Remark 6. *As $\frac{\bar{\gamma}_B}{\bar{\gamma}_E}$ tends to ∞, the asymptotic ASC is given by $\bar{C}_s \approx \hat{\mathscr{I}}_1 + \hat{\mathscr{I}}_2 - \mathscr{I}_3$, where*

$$\hat{\mathscr{I}}_1 = \sum_{k=1}^{L_E}\sum_{l=1}^{L_B}\frac{\alpha_{B,l}\alpha_{E,k}\Gamma(\beta_{E,k})}{\ln(2)\zeta_{B,l}^{\beta_{B,l}}\zeta_{E,k}^{\beta_{E,k}}}G_{2,3}^{3,1}\left[\zeta_{B,l}\middle|\begin{matrix}(0,1)\\ (0,0,\beta_{B,l})\end{matrix}\right], \tag{6.9}$$

$$\hat{\mathscr{I}}_2 = \sum_{k=1}^{L_E}\sum_{l=1}^{L_B} \frac{\alpha_{B,l}\alpha_{E,k}}{\ln(2)\beta_{B,l}\zeta_{E,k}^{\beta_{E,k}+\beta_{B,l}}} G_{2,3}^{3,1}\left[\zeta_{E,k}\left|\begin{matrix}(0,1)\\(0,0,\beta_{B,l}+\beta_{E,k})\end{matrix}\right.\right]. \tag{6.10}$$

Proof. Motivated by (Lei *et al.*, 2017a, Sec. IV), as $\frac{\bar{\gamma}_B}{\bar{\gamma}_E} \to \infty$, we have $\frac{\zeta_{E,k}}{\zeta_{B,l}} \to \infty$. Next, using the residue theorem, $\mathscr{I}_1$ is further evaluated at the simple residue 0 of the Mellin-Barnes integrand function regarding $\frac{\zeta_{E,k}}{\zeta_{B,l}}$. Then after some simple manipulations, we get $\hat{\mathscr{I}}_1$. Similarly, $\frac{\zeta_{B,l}}{\zeta_{E,k}} \to 0$, $\mathscr{I}_2$ is evaluated at the simple residue $\beta_{B,l}$, and results in $\hat{\mathscr{I}}_2$. □

6.5 Numerical Result and Discussions

In this section, the accuracy of our derived analytical results is validated. Since the MG distribution is regarded as a general model to characterize the received SNRs, three examples listed in Table 6.1 are henceforth used to correspondingly plot the Monte-Carlo simulated SOP, PNZ, and ASC.

Table 6.1 Simulations parameters

Distribution	**Parameters**, $\alpha_l = \frac{\theta_l}{\sum_{k=1}^{L_i}\theta_k\Gamma(\beta_k)\zeta_k^{-\beta_k}}$, $\bar{\gamma}_i$ is the average SNR.
$\mathscr{K}_G$ (Atapattu *et al.*, 2011, Sec. III.B), m_i and k_i are distribution shaping parameters, $L_B = L_E = 5$.	$\beta_l = m_i$, $\zeta_l = \frac{\lambda}{t_l}$, $\lambda = \frac{k_i m_i}{\bar{\gamma}_i}$, $\theta_l = \frac{\lambda^{m_i} w_l t_l^{k_i-m_i-1}}{\Gamma(m_i)\Gamma(k_i)}$, t_l, w_l are the abscissas and weight factors for the Gaussian-Laguerre integration (Abromowitz, M. & Stegun, I. A., 1968, Table 25.9).
Nakagami-n (Rician) (Atapattu *et al.*, 2011, Sec. III.F), $0 \le n < \infty$, $L_B = L_E = 20$	$\beta_l = l$, $\zeta_l = \frac{(1+n_i^2)}{\bar{\gamma}_i}$, $\theta_l = \frac{(1+n_i^2)}{\exp(n_i^2)[(l-1)!]^2\bar{\gamma}_i}\left(\frac{n_i^2(1+n_i^2)}{\bar{\gamma}_i}\right)^{l-1}$
Nakagami-q (Hoyt) (Atapattu *et al.*, 2011, Sec. III.D), $0 < q < 1$, $L_B = L_E = 5$	$\beta_l = 2l-1$, $\zeta_l = \frac{(1+q_i^2)^2}{4q_i^2\bar{\gamma}_i}$, $\theta_l = \frac{(1+q_i^2)}{2q_i\bar{\gamma}_i\Gamma(l)(l-1)!}\left(\frac{1-q_i^4}{8q_i^2\bar{\gamma}_i}\right)^{2i-2}$

Fig. 6.1 plots the SOP against $\bar{\gamma}_B$ over $\mathscr{K}_G$ fading channels for selected values of $m_B, m_B \in \{1, 1.5, 2, 2.5\}$. From this figure, one can observe that (i) our analytical results perfect the contributions in Lei *et al.* (2016c); (ii) there is a perfect agreement between our two analytical

SOP expressions respectively given by (6.3a) and (6.3b) and the corresponding simulation results; (iii) the SOP is largely enhanced with the increase of the shaping factor m_B in the high $\bar{\gamma}_B$ regime; and (iv) a larger shaping factor m_B results in a higher secrecy outage.

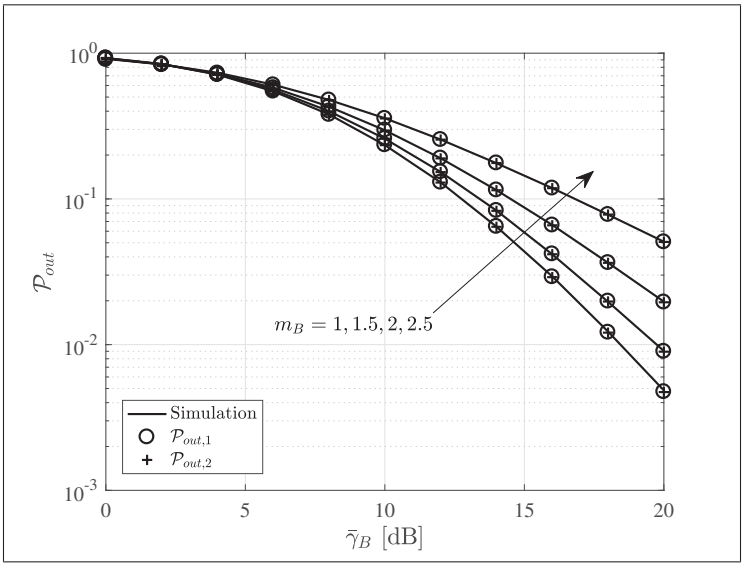


Figure 6.1 $\mathscr{P}_{out}$ versus $\bar{\gamma}_B$ over $\mathscr{K}_G$ fading channels for selected values of m_B when $R_t = 0.01$, $\bar{\gamma}_E = 6$ dB, $k_B = 4$, $m_E = 4$, and $k_E = 8$.

The lower bound of the SOP for two aforementioned cases are correspondingly depicted in Fig. 6.2. (a) and (b). It is observed that our obtained analytical lower bound for the SOP is valid for both scenarios.

In Fig. 6.3, $\mathscr{P}_{nz}$ is plotted against $\bar{\gamma}_B$ for two cases: (a) for selected values of $\bar{\gamma}_E$; (b) when the wiretap channel undergoes various fading models. Obviously, a positive secrecy capacity is ensured with a higher probability (i) either when the wiretap channel has a worse channel quality for fixed $\bar{\gamma}_B$; (ii) or when the main channel conditions gradually improve (namely, higher $\bar{\gamma}_B$) for fixed $\bar{\gamma}_E$. In addition, Fig. 6.3.(b) presents the PNZ when the main channel and wiretap channel undergo different fading models. In this vein, one can extract another interesting insight that we provide a *unified* and *general* analysis framework to analyze the PLS when the main channel and wiretap channel experience two different fading models.

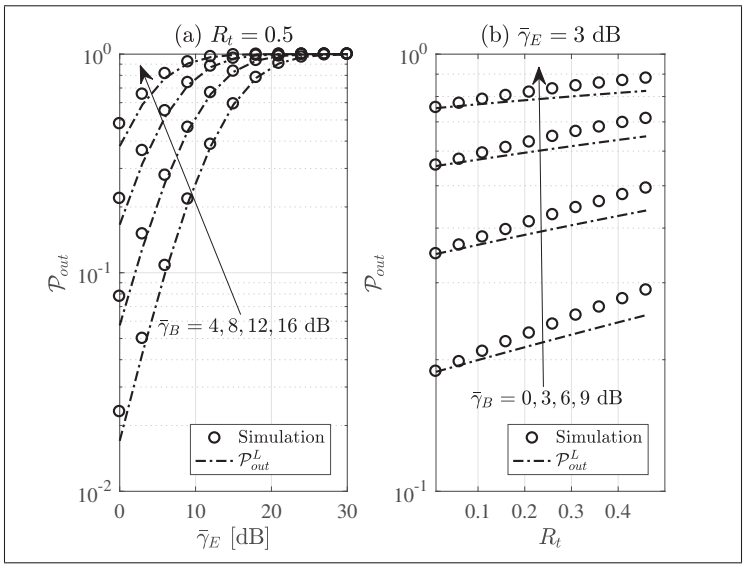


Figure 6.2 $\mathscr{P}_{out}$ versus $\bar{\gamma}_B$ over $\mathscr{K}_G$ fading channels for selected values of $k_B = 1.5, m_B = 4$, $k_E = 2.5, m_E = 8$ when (a) $R_t = 0.5$; (b) $\bar{\gamma}_E = 3$ dB.

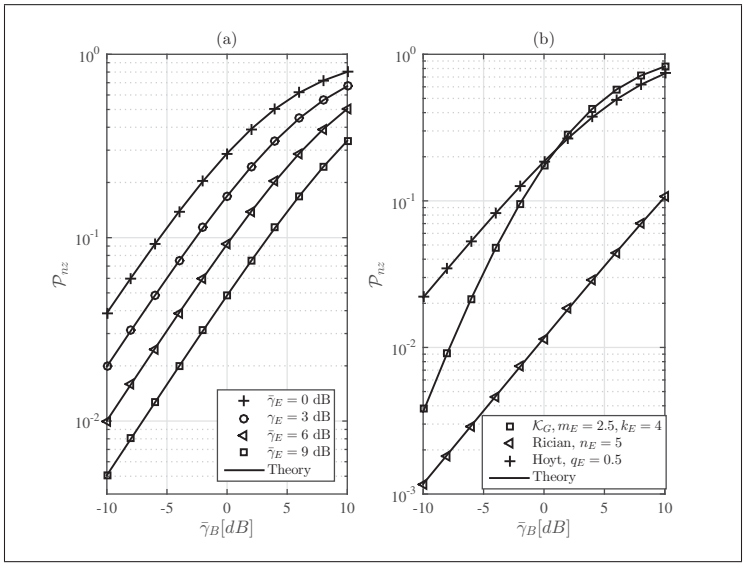


Figure 6.3 $\mathscr{P}_{nz}$ against $\bar{\gamma}_B$ for two cases: (a) main channel and wiretap channel undergo Nakagami-n fading when $n_B = 3$ and $n_E = 5$; (b) main channel undergoes $\mathscr{K}_G$ fading ($m_B = 2.5, k_B = 4$), while wiretap channel respectively undergoes $\mathscr{K}_G$, Rician, and Hoyt for $\bar{\gamma}_E = 5$ dB.

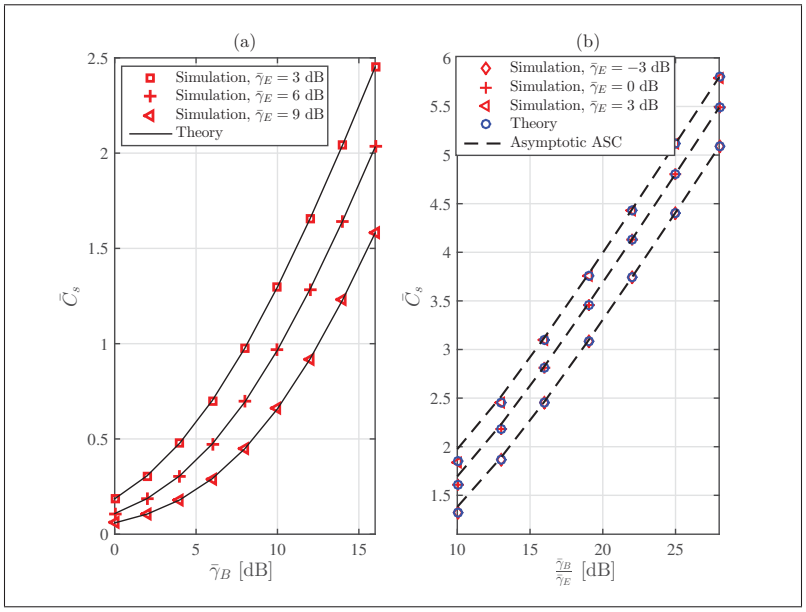


Figure 6.4 $\bar{C}_s$ over Hoyt fading channels when $q_B = q_E = \sqrt{0.5}$ for two cases (a) $\bar{C}_s$ versus $\bar{\gamma}_B$; (b) $\bar{C}_s$ versus $\frac{\bar{\gamma}_B}{\bar{\gamma}_E}$.

In continuation of verifying and comparing the exact and asymptotic ASC given in Sec. 6.4.3, Fig. 6.4 depicts how our derived ASC expression is confirmed by Monte-Carlo simulations over Hoyt fading channels. In addition, in Fig. 6.4. (b), it is shown that our asymptotic ASC accurately characterizes the exact ASC in the high $\frac{\bar{\gamma}_B}{\bar{\gamma}_E}$ regime.

6.6 Conclusion

In this letter, we first investigated PLS of wireless channels, by modeling the received SNRs as MG distributed RVs. Three secrecy metrics, i.e., SOP, PNZ, and ASC, were subsequently derived with closed-form expressions. Our derivations were validated by Monte-Carlo simulations. This paper provides a general and unified mathematical frameworks for the evaluation of the secrecy risks, especially when the instantaneous received SNRs could be rewritten in terms of the MG distribution. In addition, the obtained expressions are beneficial when the main channel and the wiretap channel undergo two different wireless channels.

CHAPTER 7

CASCADED $\alpha - \mu$ FADING CHANNELS: RELIABILITY AND SECURITY ANALYSIS

Long Kong[1], Georges Kaddoum[1], and Daniel Benevides da Costa[2]

[1] Département de Génie électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3
[2]Federal University of Ceará (UFC), Sobral-CE 62010-560, Brazil

Paper published in *IEEE ACCESS*, December, 2018.

7.1 Abstract

In this paper, the cascaded $\alpha - \mu$ fading distribution is first introduced and mathematically characterized, which arises as a generalization of the cascaded Rayleigh, Weibull, and Nakagami-m fading distribution, by properly selecting fading parameters α and μ with specific values. In particular, the statistical characterization of the cascaded $\alpha - \mu$ fading channels, namely, the probability density function (PDF) and cumulative distribution function (CDF), are first studied. This set of new statistical results is applied to the modeling and analysis of the reliability and security performance of wireless communication systems over the cascaded $\alpha - \mu$ fading channel. Regarding system reliability, the amount of fading (AoF), outage probability, average channel capacity, and the average symbol error probability (ASEP) with coherent and non-coherent demodulation schemes are derived with respect to the univariate Fox's H-function. In terms of security analysis, the secrecy outage probability $\mathscr{P}_{out}$, the probability of non-zero secrecy capacity $\mathscr{P}_{nz}$, and the average secrecy capacity are analyzed in the exact closed-form expressions which are derived in the presence of a potential eavesdropper. In addition, an asymptotic analysis of all aforementioned metrics is carried out, in order to gain more insights of the effect of the key system parameters on the reliability and security. Tractable results are computed in terms of the Fox's H-function and later on are successfully validated through Monte-Carlo simulations.

Keywords: Cascaded $\alpha - \mu$ fading channels, Fox's H-function, reliability, secrecy analysis.

7.2 Introduction

The ever-increasing demand for highly reliable wireless communication systems has led to the prosperous of various accurate channel modeling in system design and evaluation. A comprehensive summary of all existing fading models includes (i) short-term fading: Rayleigh, Rician, Nakagami-*m*, and Weibull; (ii) long-term fading: Lognormal; (iii) composite fading: Rayleigh-lognormal; and (iv) cascaded fading Boulogeorgos, A. A. A., Sofotasios, P. C., Selim, B., Muhaidat, S., Karagiannidis, G. K. & Valkama, M. (2016); Hajri, N., Youssef, N., Kawabata, T., Patzold, M. & Dahech, W. (2018); Karagiannidis *et al.* (2007); Peppas, K., Lazarakis, F., Alexandridis, A. & Dangakis, K. (2010); Sagias, N. C. & Tombras, G. S. (2007); Trigui, I., Laourine, A., Affes, S. & Stephenne, A. (2009); Yilmaz, F. & Alouini, M. S. (2009); Zheng, Z. (2015). In particular, the cascaded fading channel is mathematically based on the multiplicative modeling approach and happens over wireless communication links when 1) transmitter-and-receiver pairs experience rich scattering, but the existence of some keyholes or pinholes makes it still possible to keep the transmission; 2) the received signals are engendered by the product of a bunch of rays reflected via N statistically independent scatters.

7.2.1 Background and Related Works

Along the years, the use of cascaded fading channels has shown applicability in the modeling of several scenarios such as multi-hop cooperative communications Chergui *et al.* (2016); Ilhan, H. (2012), mobile-to-mobile (M2M) transmission channel Boulogeorgos *et al.* (2016); Erceg, V., Fortune, S. J., Ling, J., Rustako, A. J. & Valenzuela, R. A. (1997); Talha, B. & Patzold, M. (2011), dual-hop fading channels, radio-frequency identification (RFID) pinhole channels Bekkali, A., Zou, S., Kadri, A., Crisp, M. & Penty, R. V. (2015), and multiple-input-multiple-output (MIMO) keyhole communication systems Chergui *et al.* (2016); Sofotasios, P. C., Mohjazi, L., Muhaidat, S., Al-Qutayri, M. & Karagiannidis, G. K. (2016); Yilmaz & Alouini (2009).

Specifically, for M2M communication system, the double Rayleigh distribution was proposed to model it Alghorani, Y., Kaddoum, G., Muhaidat, S., Pierre, S. & Al-Dhahir, N. (2016); Boulogeorgos *et al.* (2016); Erceg *et al.* (1997). Later on, in Alghorani *et al.* (2016); Boulogeorgos *et al.* (2016), a vehicle-to-vehicle (V2V) communication scenario was investigated by characterizing the wireless links, via the $N*$Nakagami-m distribution. As shown in Karagiannidis *et al.* (2007), the $N*$Nakagami-m distribution is structured on the basis of the product of N independent, but not necessarily identical distributed Nakagami-m random variables (RVs). Its statistics, including the probability density function (PDF) and cumulative distribution function (CDF), were derived in Karagiannidis *et al.* (2007) as closed-form expressions, in terms of Meijer's G-function. The derived first-order statistics are particularly beneficial when evaluating the performance of the aforementioned various wireless communication scenarios over cascaded Nakagami-m fading channels. In addition, it is noted that the $N*$Nakagami-m distribution can be reduced to double Rayleigh by attributing $m_1 = m_2 = 1$, where m_1 and m_2 represent the fading parameters of the respective channels. However, when accounting for both short- and long-term fading effects, the $N*$Nakagami-m and $N*$Weibull distributions Sagias & Tombras (2007) cannot be adopted to model both fading impairments. As a consequence, the cascaded generalized K distribution Peppas *et al.* (2010); Trigui *et al.* (2009) was put forth to model the composite fading/shadowing channels due to the lack of closed-form expressions for the statistics of other distributions, like Suzuki Boulogeorgos *et al.* (2016); Hajri, N., Youssef, N. & Patzold, M. (2016); Laourine, A., Alouini, M. S., Affes, S. & Stephenne, A. (2009).

More recently, Yacoub proposed in Yacoub (2007a) the $\alpha - \mu$ (or, equivalently, generalized gamma) distribution to model the small scale variation of fading signal under line-of-sight conditions. It is physically described with two key fading parameters, i.e., non-linearity of the propagation medium α and the clustering of the multipath waves μ. This fading distribution has been examined applicable in vehicle communication Wu *et al.* (2010) and on-body communication networks Michalopoulou *et al.* (2012). In additon, the $\alpha - \mu$ distribution encompasses as special cases of some well-known distributions, such as Rayleigh ($\alpha = 2, \mu = 1$),

Weibull (α is the fading parameter, $\mu = 1$), and Nakagami-m ($\alpha = 2$, μ is the fading parameter) distribution, by setting appropriate fading parameters to specific values. Later on, the statistical characterization of the product of $\alpha - \mu$ variates, including its PDF and CDF, were investigated in Badarneh, O. S. & Almehmadi, F. S. (2016); Badarneh, O. S. (2016); da Silva, C. R. N., Leonardo, E. J. & Yacoub, M. D. (2018); Leonardo, E. J. & Yacoub, M. D. (2015a,1); Leonardo, E. J., Yacoub, M. D. & de Souza, R. A. A. (2016); Mathai, A. M. (1972), and the number of integers was extended from 2 to arbitrary N. The seminal results presented in Mathai (1972) were given in terms of Fox's H-function. Since the Fox's H-function is an extremely general function, taking the shape of the Mellin-Barnes integral (Mathai *et al.*, 2009a, eq. (1.2)). It can also be reduced to Meijer's G-function. However, the PDF and CDF of the product of $\alpha - \mu$ variates given in terms of hypergeometric functions is fairly complex in Leonardo & Yacoub (2015b); it renders its adoption in the performance analysis of wireless communication systems. Inspired from Leonardo & Yacoub (2015b); Mathai (1972), the objective of this paper is to regenerate the cascaded $\alpha - \mu$ distribution in terms of Fox's H-function, due to its general form and feasible implementation in MATLAB, Mathematica and Python[1].

7.2.2 Contributions

Our analysis of cascaded $\alpha - \mu$ fading channel in wireless networks will be performed in terms of reliability and security. It is noteworthy that apart from analyzing the popular average bit error ratio performance, plenty of research attention concerning the security issue is also gained when designing a secure and reliable communication system. The security issue is based on Wyner's wiretap model Wyner (1975), where the legitimate links are endangered by the malicious eavesdroppers. In the existing technical works Kong *et al.* (2016b,1); Lei

[1] The implementation of the univariate, bivariate or multivariate Fox's H-function are reported in Ansari, I. S., Yilmaz, F. & Alouini, M. S. (2013); Peppas (2012); Peppas *et al.* (2012); Yilmaz & Alouini (2009) at Mathematica, MATLAB or Python. More specifically, the univariate Fox's H-function is implemented at Mathematica in Ansari *et al.* (2013); Yilmaz & Alouini (2009), and at MATLAB in Peppas *et al.* (2012), whereas the implementation of the bivariate Fox's H-function is given at MATLAB in Peppas (2012).

et al. (2015,1), the authors studied the security problem over $\alpha - \mu$ fading channels from the perspective of information theory, in which the secrecy outage probability, the probability of non-zero secrecy capacity, and average secrecy capacity were characterized, respectively. However, no work in the open literature focused on cascaded $\alpha - \mu$ fading channels.

To this end, this paper aims to provide a reliability and security analysis of communications systems over cascaded α-μ fading channels. The main contributions can be summarized as follows:

1) The cascaded $\alpha - \mu$ distribution is first introduced. Its PDF and CDF are analyzed by first expressing the $\alpha - \mu$ distribution in terms of the Fox's H-function, and subsequently being derived by utilizing the property of the Fox's H-function distribution. In addition, other elementary statistics, including moments and moment-generating function (MGF), are also derived.

2) The derived statistics are employed in the investigation of multi-hop relaying wireless systems with amplify-and-forward (AF) protocol over the cascaded $\alpha - \mu$ fading channel. In particular,

   - In the absence of eavesdroppers, the reliability of point-to-point wireless systems is characterized. Specifically, the amount of fading (AoF), the outage probability, the average channel capacity and the average symbol error probability (ASEP) are evaluated in terms of the univariate Fox's H-function.
   - In the presence of eavesdroppers, the physical layer security is investigated, where the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), and the average secrecy capacity, are characterized and closed-form expressions in terms of the bivariate and univariate Fox's H-functions, are obtained.
   - Asymptotic behavior of all the aforementioned metrics are analyzed to gain further insights on the effect of the key system parameters on the overall performance. In addition, numerical results are conducted to confirm our analysis for both scenarios,

perfect agreements are observed to show the accuracy and feasibility of our analysis in the field of wireless communication systems.

3) The useful insight provided in our paper lies in the essence of the cascaded $\alpha-\mu$ fading channels, which can be reduced to several well-known cascaded fading channels, such as the cascaded Rayleigh, Weibull, Nakagami-*m* fading channels by fixing α and μ with special values, furthermore, the exact closed-form expression of the PDF and CDF of the cascaded $\alpha-\mu$ distribution makes it tractable to grasp the behavior of reliability and security analysis for multi-hop wireless communication systems.

The rest of this paper is organized as follows. In Section 7.3, the statistical characterization of cascaded $\alpha-\mu$ fading channel is first performed. Section 7.4 demonstrates the application of cascaded $\alpha-\mu$ fading channels in modeling wireless communication systems, and performance metrics including the outage probability, average channel capacity and the average symbol error probability (ASEP) are analyzed respectively. In Section 7.5, the physical layer security of wireless communication systems over cascaded α-μ fading channels is investigated, and performance metrics including the secrecy outage probability, the probability of non-zero secrecy capacity, and average secrecy capacity, are provided. Section 7.6 presents some illustrative numerical results along with insightful discussions. Concluding remarks and future works are outlined in Section 7.7.

Notations: $\Gamma(x)$ denotes the Gamma function (Gradshteyn & Ryzhik, 2014, eq. (8.310.1)), $\Gamma(a,x)$ is the upper incomplete gamma function, $H_{p,q}^{m,n}[.]$ is the univariate Fox's H-function (Mathai *et al.*, 2009a, eq. (1.2)), $H_{p,q:p_1,q_1:p_2,q_2}^{0,n:m_1,n_1:m_2,n_2}$ is the bivariate Fox's H-function (Mathai *et al.*, 2009a, eq. (2.56)). erfc$(.)$ is the complementary error function. $\mathscr{B}(x,y)$ is the Beta function (Gradshteyn & Ryzhik, 2014, eq. (8.380.1)). $\psi(\cdot)$ is the digamma function. $G_{p,q}^{m,n}[.]$ is the Meijer's G-function (Gradshteyn & Ryzhik, 2014, eq. (7.811.1)). $\mathscr{M}[f(x),s]$ denotes the Mellin transform of $f(x)$ (Debnath & Bhatta, 2014, eq. (8.2.5)), $\mathbb{E}(\cdot)$ and $\mathbb{V}(\cdot)$ mean expectation and variance, respectively. Res$[f(x),p]$ represents the residue of function $f(x)$ at pole $x=p$.

7.3 System Model and Statistical Characterization

Let Z be the product of $M, M \geq 1$ independently $\alpha-\mu$ distributed random variables (RVs) having parameters (α_i, μ_i), i.e., $Z = \prod_{i=1}^{M} R_i$, the PDF of R_i is given by Yacoub (2007a)

$$f_{R_i}(r_i) = \frac{\alpha_i \mu_i^{\mu_i} r_i^{\alpha_i \mu_i - 1}}{\Omega_i^{\alpha_i \mu_i} \Gamma(\mu_i)} \exp\left(-\mu_i \left(\frac{r_i}{\Omega_i} \right)^{\alpha_i} \right) = \tau_i H_{0,1}^{1,0}\left[\upsilon_i r_i \middle| \begin{matrix} - \\ (\mu_i - \frac{1}{\alpha_i}, \frac{1}{\alpha_i}) \end{matrix} \right], \tag{7.1}$$

where $\tau_i = \frac{\mu_i^{\frac{1}{\alpha_i}}}{\Omega_i \Gamma(\mu_i)}$, $\upsilon_i = \frac{\mu_i^{\frac{1}{\alpha_i}}}{\Omega_i}$, $\Omega_i = \frac{\Gamma(\mu_i)}{\Gamma(\mu_i + \frac{2}{\alpha_i})}$, the last step holds by using (Mathai *et al.*, 2009a, eq. (1.125)).

Theorem 14. *The PDF of Z is given by*

$$f_Z(z) = \mathscr{D}_M H_{0,M}^{M,0}\left[\mathscr{V}_M z \middle| \begin{matrix} - \\ \varepsilon_1, \cdots, \varepsilon_M \end{matrix} \right], \tag{7.2}$$

where $\mathscr{D}_M = \prod_{i=1}^{M} \tau_i$, $\mathscr{V}_M = \prod_{i=1}^{M} \upsilon_i$, $\varepsilon_i = (\mu_i - \frac{1}{\alpha_i}, \frac{1}{\alpha_i})$.

Proof. By using (Bodenschatz, 1992, eq. (3.12)), the proof is easily obtained. □

7.3.1 System Model

Suppose a wireless multi-hop amplify-and-forward relaying communication link, shown in Fig. 7.1, over cascaded $\alpha-\mu$ fading channel. It is assumed that each hop undergoes the $\alpha-\mu$ fading with fading coefficient h_i, and h_i is characterized with fading parameters α_i and μ_i. The instantaneous received signal-to-noise ratio (SNR) at the desired destination is expressed as

$$\gamma = \prod_{i=1}^{N} \bar{\gamma} g_i, \tag{7.3}$$

where $\bar{\gamma}$ is the average power at the receiver side, $g_i = |h_i|^2$, and h_i is the fading coefficient, which follows independent and non-identically $\alpha-\mu$ distribution with parameters (α_i, μ_i). It

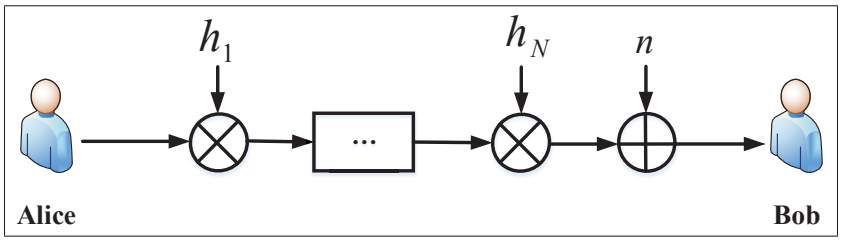


Figure 7.1 Cascaded fading channels with N components

is assumed that all h_i are statistically independent, but not necessarily identically distributed. The PDF of g_i is defined in (Kong *et al.*, 2016b,1, eq. (2)) and given by

$$f_g(g_i) = \frac{\alpha_i g_i^{\frac{\alpha_i\mu_i}{2}-1}}{2\Omega_i^{\frac{\alpha_i\mu_i}{2}}\Gamma(\mu_i)} \exp\left[-\left(\frac{g_i}{\Omega_i}\right)^{\frac{\alpha_i}{2}}\right] \overset{(a)}{=} \kappa_i H_{0,1}^{1,0}\left[\lambda_i g_i \middle| \begin{matrix} - \\ \Phi_i \end{matrix}\right], \tag{7.4}$$

where $\Omega_i = \frac{\Gamma(\mu_i)}{\Gamma(\mu_i+\frac{2}{\alpha_i})}$, $\kappa_i = \frac{1}{\Omega_i\Gamma(\mu_i)}$, $\lambda_i = \frac{1}{\Omega_i}$, and $\Phi_i = (\mu_i - \frac{2}{\alpha_i}, \frac{2}{\alpha_i})$. Step (a) is derived by using (Mathai *et al.*, 2009a, eq. (1.125)).

7.3.2 Statistical Characterization

Theorem 15. *The PDF and CDF of the instantaneous SNR defined in (7.3) can be expressed as*

$$f_\gamma(\gamma) = \mathscr{K}_N H_{0,N}^{N,0}\left[\mathscr{C}\gamma \middle| \begin{matrix} - \\ \Phi_1,\cdots,\Phi_N \end{matrix}\right], \tag{7.5a}$$

$$F_\gamma(\gamma) = 1 - \frac{\mathscr{K}_N}{\mathscr{C}} H_{1,N+1}^{N+1,0}\left[\mathscr{C}\gamma \middle| \begin{matrix} (1,1) \\ (0,1),\theta_1,\cdots,\theta_N \end{matrix}\right] = 1 - \bar{F}_\gamma(\gamma), \tag{7.5b}$$

where $\mathscr{K}_N = \frac{\prod_{i=1}^N \kappa_i}{\bar{\gamma}}$, $\mathscr{C} = \frac{\prod_{i=1}^N \lambda_i}{\bar{\gamma}}$, $\theta_i = (\mu_i, \frac{2}{\alpha_i})$, *and* $\bar{F}_\gamma$ *is the complementary CDF (CCDF) of* F_γ.

Proof. Let Z be the product of N mutually independent and non-identically random variables (RVs) $g_1, g_2, \cdots, g_N$, that is

$$Z = \frac{\gamma}{\bar{\gamma}} = \prod_{i=1}^{N} g_i. \tag{7.6}$$

Since α-μ distribution is a special case of the Fox's H-function distribution, by using the transformation property of Fox's H-function (Bodenschatz, 1992, eq. (3.12)) and $f_\gamma(\gamma) = \frac{1}{\bar{\gamma}} f_Z\left(\frac{z}{\bar{\gamma}}\right)$, the proof for (7.5a) is easily obtained. Afterwards, by applying (Bodenschatz, 1992, eq. (3.7)), the CDF is subsequently achieved. □

Remark 7. The PDF of the ratio of two instantaneous SNRs, $Y = \frac{\gamma_1}{\gamma_2}$, respectively defined in (7.3), i.e., $\gamma_1 = \prod_{i=1}^{N_1} \bar{\gamma}_1 g_{1,i}$, and $\gamma_2 = \prod_{i=1}^{N_2} \bar{\gamma}_2 g_{2,i}$ is given by

$$f_{\frac{\gamma_1}{\gamma_2}}(y) = \frac{\mathscr{K}_{N_1}\mathscr{K}_{N_2}}{\mathscr{C}_{N_2}^2} H_{N_2,N_1}^{N_1,N_2}\left[\frac{\mathscr{C}_{N_1}}{\mathscr{C}_{N_2}} y \,\middle|\, \begin{matrix} \Theta_1, \cdots, \Theta_{N_2} \\ \Phi_1, \cdots, \Phi_{N_1} \end{matrix}\right], \tag{7.7}$$

where $\Theta_n = \left(1 - \mu_i - \frac{2}{\alpha_i}, \frac{2}{\alpha_i}\right), n = 1, \cdots, N_2$.

Proof. Using (Bodenschatz, 1992, Eq. (3.14)), and after some simple mathematical manipulations, the proof is easily achieved. □

As shown in Fig. 7.2, examples of PDFs for (7.5a) and (7.7) are plotted, one can observe that there is a perfect match between the Monte-Carlo simulation results and our analysis.

For the conveniences of the following performance analysis, the definition of Mellin transform for a continuous function $f(x)$ is recalled, which is given by

$$\mathscr{M}[f(x), s] = \int_0^\infty f(x) x^{s-1} dx. \tag{7.8}$$

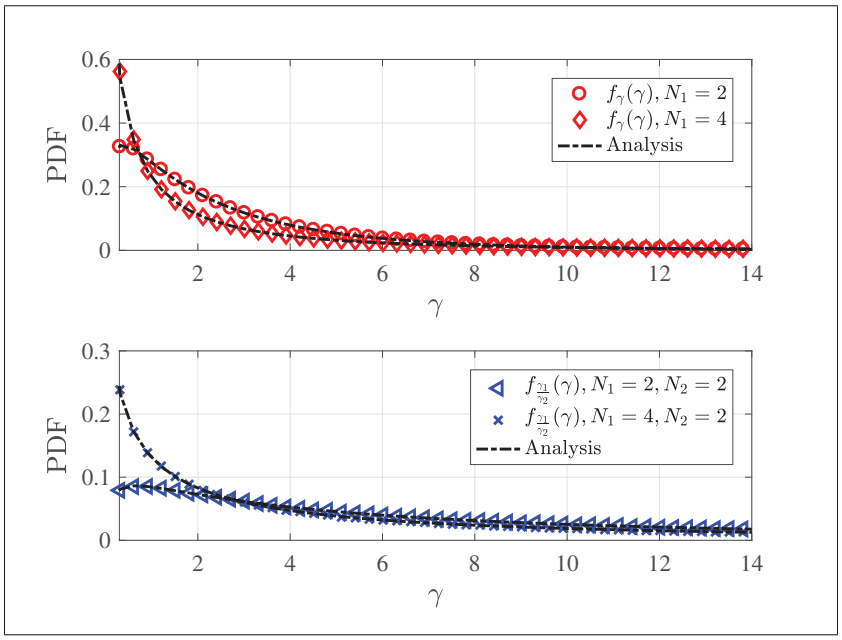


Figure 7.2 PDFs of $\gamma = \prod_{k=1}^{N} \bar{\gamma} g_k$ and the ratio of $\gamma = \frac{\gamma_1}{\gamma_2}$, where $\gamma_1 = \prod_{k=1}^{N_1} \bar{\gamma}_1 g_{1,i}$, $\gamma_2 = \prod_{i=1}^{N_2} \bar{\gamma} g_{2,i}$, $g_k, g_{1,i}, g_{2,i}$ are implemented by using the WAFO toolbox Brodtkorb *et al.* (2000) when $\bar{\gamma} = \bar{\gamma}_1 = 5$ dB and $\bar{\gamma}_2 = -5$ dB

Likewise, the Mellin transform for (7.5a) is straightforward given from (Mathai *et al.*, 2009a, eq. (2.8))

$$\mathscr{M}[f_\gamma(\gamma), s] = \frac{\mathscr{K}_N \prod_{i=1}^{N} \Gamma\left(\mu_i - \frac{2}{\alpha_i} + \frac{2}{\alpha_i} s\right)}{\mathscr{C}_N^s}. \tag{7.9}$$

7.3.3 Moments and MGF

The n-th moment of the instantaneous SNR can be derived from the following definition,

$$\mathbb{E}[\gamma^n] = \int_0^\infty x^n f_\gamma(x) dx, \tag{7.10}$$

it can be achieved by using the Mellin transform of the Fox's H-function(Prudnikov *et al.*, 1990, eq. (2.25.2.1)), and thus given by

$$\mathbb{E}[\gamma^n] = \frac{\mathscr{K}_N \prod_{i=1}^{N} \Gamma\left(\mu_i + \frac{2}{\alpha_i} n\right)}{\mathscr{C}_N^{n+1}}. \tag{7.11}$$

Likewise, the MGF of the received SNR γ, is defined by

$$\mathbb{M}_\gamma(-s) = \int_0^\infty \exp(-xs) f_\gamma(x) dx, \tag{7.12}$$

it can be derived by re-expressing the $\exp(\cdot)$ function through its Fox's H-function form Prudnikov *et al.* (1990), namely,

$$\exp(-x) = H_{0,1}^{1,0}\left[x \middle| \begin{matrix} - \\ (0,1) \end{matrix}\right],$$

and then making use of the Mellin transform of the product of two Fox's H-functions (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), yields

$$\mathbb{M}_\gamma(-s) = \frac{\mathscr{K}_N}{s} H_{1,N}^{N,1}\left[\frac{\mathscr{C}}{s} \middle| \begin{matrix} (0,1) \\ \Phi_1, \cdots, \Phi_N \end{matrix}\right]. \tag{7.13}$$

7.4 Reliability Analysis over Cascaded $\alpha - \mu$ Fading Channels

In this section, the objective is to evaluate the link performance, as shown in Fig. 7.1, when no eavesdropper is taken into account. The AoF, the outage probability, average channel capacity, and average symbol error probability are analyzed and derived in terms of the univariate Fox's H-function, respectively. In addition, their asymptotic behavior is given by using the residue approach given in (Chergui *et al.*, 2016, Sec. IV).

7.4.1 Amount of Fading

The AoF is defined as the ratio of the variance to the square average SNR, and then using (7.11), we have

$$AF = \frac{\mathbb{V}(\gamma)}{\mathbb{E}^2(\gamma)} = \frac{\mathbb{E}(\gamma^2)}{\mathbb{E}(\gamma)^2} - 1 = \frac{\mathscr{C}_N}{\mathscr{K}_N} \frac{\prod_{i=1}^{N} \Gamma\left(\mu_i + \frac{4}{\alpha_i}\right)}{\prod_{i=1}^{N} \Gamma\left(\mu_i + \frac{2}{\alpha_i}\right)^2} - 1. \tag{7.14}$$

7.4.2 Outage Probability

The outage event happens when the output SNR falls below a given threshold γ_{th}, which can be expressed mathematically as

$$\mathscr{P}_{op}(\gamma_{th}) = Pr(\gamma < \gamma_{th}). \tag{7.15}$$

7.4.2.1 Exact Analysis

By applying (7.5b), the outage probability is given by

$$\mathscr{P}_{op}(\gamma_{th}) = 1 - \frac{\mathscr{K}_N}{\mathscr{C}} H_{1,N+1}^{N+1,0}\left[\mathscr{C}\gamma_{th} \middle| \begin{matrix} (1,1) \\ (0,1), \theta_1, \cdots, \theta_N \end{matrix}\right]. \tag{7.16}$$

7.4.2.2 Asymptotic Analysis

When $\frac{\gamma_{th}}{\bar{\gamma}} \to \infty$, by using the residue approach, the asymptotic behavior of (7.16) is given by

$$\mathscr{P}_{op} \sim 1 - \frac{\mathscr{K}_N}{\mathscr{C}} \prod_{i=1}^{N} \Gamma(\mu_i). \tag{7.17}$$

Proof. See Appendix. III.1. □

7.4.3 Average Channel Capacity

The average channel capacity over fading channels is computed by averaging the instantaneous channel capacity

$$\bar{C} = \int_0^{\infty} \log_2(1+\gamma) f_{\gamma}(\gamma) d\gamma. \tag{7.18}$$

7.4.3.1 Exact Analysis

Theorem 16. *The average channel capacity over cascaded $\alpha-\mu$ fading channels is given by*

$$\bar{C} = \frac{\mathscr{K}_N}{\mathscr{C}\ln(2)} H_{2,N+2}^{N+2,1}\left[\mathscr{C}\left|\begin{matrix}(0,1),(1,1)\\(0,1),(0,1),\theta_1,\cdots,\theta_N\end{matrix}\right.\right]. \tag{7.19}$$

Proof. By applying the Parseval's relation for the Mellin transform on (7.18), we have

$$\bar{C} = \frac{1}{2\pi j}\int_{\mathscr{L}} \mathscr{M}[\log_2(1+\gamma),1-s]\mathscr{M}[f(\gamma),s]ds, \tag{7.20}$$

where $j=\sqrt{-1}$, $\mathscr{L}$ is the integration path from $\upsilon - j\infty$ to $\upsilon + j\infty$, υ is a constant, and

$$\mathscr{M}[\log_2(1+\gamma),1-s] = \frac{\Gamma(2-s)\Gamma(s-1)\Gamma(s-1)}{\ln(2)\Gamma(s)}, \tag{7.21a}$$

$$\mathscr{M}[f(\gamma),s] = \mathscr{K}\prod_{i=1}^{N}\Gamma\left(\mu_i - \frac{2}{\alpha_i} + \frac{2}{\alpha_i}s\right)\mathscr{C}^{-s}. \tag{7.21b}$$

After plugging (7.21a) and (7.21b) into (7.20), leading to the following result

$$\begin{aligned}\bar{C} &= \frac{\mathscr{K}_N}{2\ln(2)\pi i}\int_{\mathscr{L}} \frac{\Gamma(2-s)\Gamma(s-1)\Gamma(s-1)}{\Gamma(s)}\prod_{i=1}^{N}\Gamma\left(\mu_i - \frac{2}{\alpha_i} + \frac{2}{\alpha_i}s\right)\mathscr{C}^{-s}ds \\ &\overset{(b)}{=} \frac{\mathscr{K}_N}{\ln(2)} H_{2,N+2}^{N+2,1}\left[\mathscr{C}\left|\begin{matrix}(-1,1),(0,1)\\(-1,1),(-1,1),\Phi_1,\cdots,\Phi_N\end{matrix}\right.\right],\end{aligned} \tag{7.22}$$

where step (b) is developed by applying the definition of univariate Fox's H-function, and subsequently using (Mathai *et al.*, 2009a, eq. (1.60)), the proof is completed. □

7.4.3.2 Asymptotic Analysis

At high SNR regime, by using the residue approach (Kong *et al.*, 2016b, Sec. IV), (7.19) can be easily determined as

$$\bar{C} \sim \frac{\mathscr{K}_N \prod_{i=1}^{N} \Gamma(\mu_i)}{\mathscr{C} \ln(2)} \left[\sum_{i=1}^{N} \frac{2}{\alpha_i} \psi(\mu_i) - \ln(\mathscr{C}) \right]. \tag{7.23}$$

7.4.4 Average Symbol Error Probability (ASEP)

Apart from the aforementioned two metrics, the average symbol error probability is considered as another crucial criterion when designing reliable transmission system. It is defined as follows

$$\bar{\mathscr{P}}_{se}^{k} = \int_0^{\infty} \mathscr{P}_{se}^{k}(\gamma) f_{\gamma}(\gamma) d\gamma, \tag{7.24}$$

where $k \in \{C, N\}$, $\mathscr{P}_{se}(\gamma)$ is the conditional error probability with different generic expressions for coherent and non-coherent modulation schemes, which are listed in Tables. 7.1 and 7.2 Badarneh, O. S. & Aloqlah, M. S. (2016), respectively.

Table 7.1 Values of a, b for different modulation schemes by using coherent demodulation where $\mathscr{P}_{se}^{C} = a \operatorname{erfc}(\sqrt{b\gamma})$

Modulation Scheme	a	b
BPSK	$\frac{1}{2}$	1
BFSK	$\frac{1}{2}$	$\frac{1}{2}$
QPSK, 4-QAM	1	$\frac{1}{2}$
M-QAM ($M \geq 4$)	$\frac{2(\sqrt{M}-1)}{\sqrt{M}}$	$\frac{3}{2(M-1)}$

Table 7.2 Values of a, b for different modulation schemes by using non-coherent demodulation where $\mathscr{P}_{se}^{N} = a\exp(-b\gamma)$

Modulation Scheme	a	b
BFSK	$\frac{1}{2}$	$\frac{1}{2}$
DBPSK	$\frac{1}{2}$	1

7.4.4.1 Exact Analysis

Theorem 17. *The average ASEP over cascaded α-μ fading channels by using coherent and non-coherent demodulation are respectively given by*

- *Coherent Demodulation*

$$\bar{\mathscr{P}}_{se}^{C} = \frac{a\mathscr{K}}{\mathscr{C}\sqrt{\pi}} H_{2,N+1}^{N,2}\left[\frac{\mathscr{C}}{b}\middle|\begin{matrix}(1,1),(\frac{1}{2},1)\\ \theta_1,\cdots,\theta_N,(0,1)\end{matrix}\right], \tag{7.25}$$

- *Non-coherent Demodulation*

$$\bar{\mathscr{P}}_{se}^{N} = \frac{a\mathscr{K}}{b} H_{1,N}^{N,1}\left[\frac{\mathscr{C}}{b}\middle|\begin{matrix}(0,1)\\ \Phi_1,\cdots,\Phi_N\end{matrix}\right]. \tag{7.26}$$

Proof. Re-expressing $\mathscr{P}_{se}^{C}$ in terms of the Fox's H-function (Prudnikov *et al.*, 1990, eq. (8.4.14.2)), we have

$$\mathscr{P}_{se}^{C} = a\ \mathrm{erfc}(\sqrt{b\gamma}) = \frac{a}{\sqrt{\pi}} H_{1,2}^{2,0}\left[b\gamma\middle|\begin{matrix}(1,1)\\ (0,1),(\frac{1}{2},1)\end{matrix}\right], \tag{7.27}$$

Next, applying the Parseval's relation for Mellin transform of (7.24), yields the following result

$$\bar{\mathscr{P}}_{se}^{C} = \int_0^{\infty} \mathscr{P}_{se}^{C}(\gamma) f_{\gamma}(\gamma) d\gamma = \frac{a}{2\pi^{\frac{3}{2}} i} \int_{\mathscr{L}} \mathscr{M}[\mathrm{erfc}(\sqrt{b\gamma}), 1-s]\mathscr{M}[f_{\gamma}(\gamma), s] ds, \tag{7.28}$$

where $\mathscr{M}[\text{erfc}(\sqrt{b\gamma}), 1-s]$ can be obtained from (Prudnikov *et al.*, 1990, eq. (8.4.14.2)) and is given by

$$\mathscr{M}[\text{erfc}(\sqrt{b\gamma}), 1-s] = \frac{\Gamma(1-s)\Gamma\left(\frac{3}{2}-s\right)}{\Gamma(2-s)} b^{-(1-s)}. \tag{7.29}$$

Subsequently, substituting (7.29) and (7.21b) into (7.28), and then applying the definition of Fox's H-function, we have

$$\begin{aligned} \bar{\mathscr{P}}_{se}^{C} &= \frac{a\mathscr{K}}{2b\pi^{\frac{3}{2}} i} \int_{\mathscr{L}} \frac{\Gamma(1-s)\Gamma\left(\frac{3}{2}-s\right)}{\Gamma(2-s)} \prod_{i=1}^{N} \Gamma\left(\mu_i - \frac{2}{\alpha_i} + \frac{2}{\alpha_i} s\right) \left(\frac{\mathscr{C}}{b}\right)^{-s} ds \\ &= \frac{a\mathscr{K}}{b\sqrt{\pi}} H_{2,N+1}^{N,2} \left[\frac{\mathscr{C}}{b} \middle| \begin{matrix} (0,1), (-\frac{1}{2}, 1) \\ \Phi_1, \cdots, \Phi_N, (-1,1) \end{matrix} \right]. \end{aligned} \tag{7.30}$$

Finally, using the property of Fox's H-function (Mathai *et al.*, 2009a, eq. (1.60)), the proof for (7.25) is accomplished.

Regarding the proof for (7.26), by providing the Mellin transform for the exponential function (Prudnikov *et al.*, 1990, eq.(8.4.3.1)) as follows,

$$\mathscr{M}[\exp(-b\gamma), 1-s] = \frac{\Gamma(1-s)}{b^{(1-s)}}, \tag{7.31}$$

and then following the same steps from (7.28) to (7.30), as such, the proof is achieved. □

7.4.4.2 Asymptotic Analysis

At high $\bar{\gamma}$ regime, the asymptotic behavior of (7.25) and (7.26) can be likely obtained as follows by following the same method as shown in Appendix. 1 Kong *et al.* (2016b)

- Coherent Demodulation

$$\bar{\mathscr{P}}_{se}^{C} \sim \frac{a\mathscr{K}\left(\frac{\mathscr{C}}{b}\right)^{\frac{\alpha_j \mu_j}{2}}}{\mu_j \sqrt{\pi} \mathscr{C}} \Gamma\left(\frac{1+\alpha_j \mu_j}{2}\right) \prod_{i=1,}^{N-1} \Gamma\left(\mu_i - \frac{\alpha_j}{\alpha_i} \mu_j\right), \tag{7.32}$$

- Non-coherent Demodulation

$$\bar{\mathscr{P}}_{se}^{N} \sim \frac{a\mathscr{K}\left(\frac{\mathscr{C}}{b}\right)^{\frac{\alpha_j\mu_j}{2}}}{\sqrt{\pi}\mathscr{C}}\Gamma\left(\frac{\alpha_j\mu_j}{2}\right)\prod_{i=1,}^{N-1}\Gamma\left(\mu_i-\frac{\alpha_j}{\alpha_i}\mu_j\right), \tag{7.33}$$

where $\alpha_j\mu_j = \min(\alpha_i\mu_i), i = 1,\cdots,N$.

7.5 Secrecy Analysis over Cascaded $\alpha-\mu$ Fading Channels

In this section, the security issue over cascaded $\alpha-\mu$ fading channels is analyzed from the information theoretical perspective. The classic Wyner's wiretap channel model is deployed, where a transmitter, named Alice, intends to communicate with the legitimate destination, Bob, whilst encountering a malicious wiretapper, Eve, over the cascaded $\alpha-\mu$ fading channels, a possible system configuration is shown in Fig. 7.3. It is assumed that (i) all users are equipped with a single antenna; (ii) they have perfect knowledge of their channel state information (CSI); (iii) the main channel is independent of the wiretap channel.

7.5.1 System Model

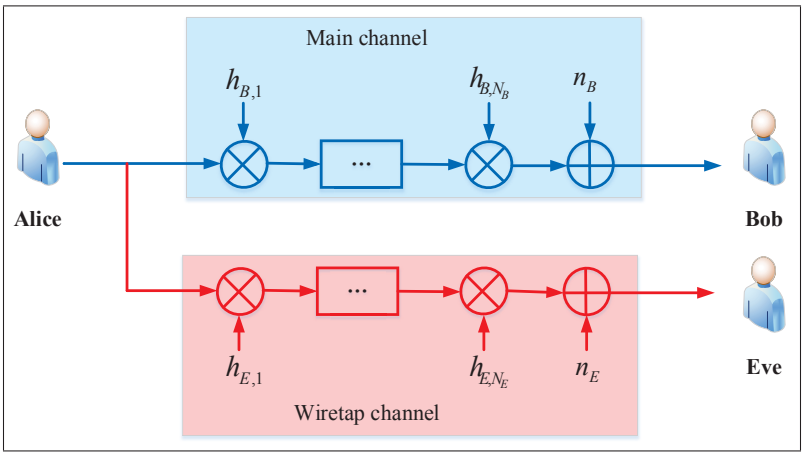


Figure 7.3 Cascaded $\alpha-\mu$ fading channels in the presence of a potential eavesdropper

Suppose a wireless legitimate link, from Alice to Bob, undergoes the cascaded fading channels while in the presence of a potential Eve, where the channel coefficients are modeled by independent $\alpha-\mu$ distributions. The link between Alice and Bob is named as the main channel, whereas the one between Alice and Eve is called the wiretap channel. As a consequence, the instantaneous SNRs at Bob and Eve can be respectively expressed as

$$\gamma_B = \prod_{i=1}^{N_B} \bar{\gamma}_B g_{B,i}, \tag{7.34a}$$

$$\gamma_E = \prod_{j=1}^{N_E} \bar{\gamma}_E g_{E,j}, \tag{7.34b}$$

where $\bar{\gamma}_B = \frac{P}{\sigma_B}$ and $\bar{\gamma}_E = \frac{P}{\sigma_E}$, $g_{B,i} = |h_{B,i}|^2$, $g_{E,j} = |h_{E,j}|^2$, P, σ_B and σ_E are the transmission power at Alice, the noise power at Bob and Eve, respectively.

By deploying Theorem 15 on γ_B and γ_E, $f_B(\gamma_B)$ and $f_E(\gamma_E)$ are respectively given by

$$f_B(\gamma_B) = \mathscr{K}_{N_B} H_{0,N_B}^{N_B,0}\left[\mathscr{C}_{N_B}\gamma_B \,\middle|\, \begin{matrix} - \\ \Phi_1,\cdots,\Phi_{N_B} \end{matrix}\right], \tag{7.35a}$$

$$f_E(\gamma_E) = \mathscr{K}_{N_E} H_{0,N_E}^{N_E,0}\left[\mathscr{C}_{N_E}\gamma_E \,\middle|\, \begin{matrix} - \\ \Theta_1,\cdots,\Theta_{N_E} \end{matrix}\right], \tag{7.35b}$$

where $\begin{cases} \mathscr{K}_{N_B} = \frac{\prod_{i=1}^{N_B} \kappa_{B,i}}{\bar{\gamma}_B} \\ \Phi_i = \left(\mu_{B,i} - \frac{2}{\alpha_{B,i}}, \frac{2}{\alpha_{B,i}}\right), \quad i = 1,\cdots,N_B, \\ \mathscr{C}_{N_B} = \frac{\prod_{i=1}^{N_B} \lambda_{B,i}}{\bar{\gamma}_B} \end{cases}$

and $\begin{cases} \mathscr{K}_{N_E} = \frac{\prod_{j=1}^{N_E} \kappa_{B,j}}{\bar{\gamma}_E} \\ \Theta_j = \left(\mu_{E,j} - \frac{2}{\alpha_{E,j}}, \frac{2}{\alpha_{E,j}}\right), \quad j = 1,\cdots,N_E\,. \\ \mathscr{C}_{N_E} = \frac{\prod_{j=1}^{N_E} \lambda_{E,j}}{\bar{\gamma}_E} \end{cases}$

According to Bloch *et al.* (2008), the instantaneous secrecy capacity is mathematically defined as the difference of the instantaneous capacity of the main channel and wiretap channel, given as follows

$$C_s = \begin{cases} C_M - C_W, & \gamma_B > \gamma_E \\ 0, & \text{otherwise.} \end{cases} \tag{7.36}$$

where $C_M = \log_2(1+\gamma_B)$, $C_W = \log_2(1+\gamma_E)$.

7.5.2 Secrecy Outage Probability

The secrecy outage probability $\mathscr{P}_{out}$ is defined as the probability with an instantaneous secrecy capacity, C_s, falling down the target secrecy rate R_t.

Revisiting (7.36), the secrecy outage probability $\mathscr{P}_{out}$ for the Wyner's wiretap fading model is conceptually explained through two cases: (i) $C_s < R_s$ whilst positive secrecy capacity is guaranteed; (ii) $P_{out}(R_s)$ definitely happens when the secrecy capacity is non-positive Kong *et al.* (2016a). $\mathscr{P}_{out}(R_s)$ can thus be rewritten as follows:

$$\begin{aligned} \mathscr{P}_{out}(R_t) &= \mathscr{P}r(C_s < R_t) = \mathscr{P}r(\gamma_B \leq R_s\gamma_E + R_s - 1) \\ &= \mathscr{P}r(C_s < R_s|\gamma_B > \gamma_E)\mathscr{P}r(\gamma_B > \gamma_E) + \mathscr{P}r(\gamma_B < \gamma_E) \\ &= \int_0^\infty \int_{\gamma_E}^{\gamma_0} f_B(\gamma_B) f_E(\gamma_E) d\gamma_B d\gamma_E + \int_0^\infty \int_0^{\gamma_E} f_B(\gamma_B) f_E(\gamma_E) d\gamma_B d\gamma_E \\ &= \int_0^\infty f_E(\gamma_E) \left[\int_0^{\gamma_0} - \int_0^{\gamma_E} \right] f_B(\gamma_B) d\gamma_B d\gamma_E + \int_0^\infty \int_0^{\gamma_E} f_B(\gamma_B) f_E(\gamma_E) d\gamma_B d\gamma_E \\ &= \int_0^\infty F_B(\gamma_0) f_E(\gamma_E) d\gamma_E = 1 - \int_0^\infty \bar{F}_B(\gamma_0) f_E(\gamma_E) d\gamma_E, \end{aligned} \tag{7.37}$$

where $\gamma_0 = 2^{R_t}\gamma_E + 2^{R_t} - 1 = R_s\gamma_E + \mathscr{W}$, $R_s = 2^{R_t}, \mathscr{W} = 2^{R_t} - 1$, and with the help of (7.5b), we have

$$\bar{F}_B(\gamma_0) = \frac{\mathscr{K}_{N_B}}{\mathscr{C}_{N_B}} H_{1,N_B+1}^{N_B+1,0} \left[\mathscr{C}_{N_B}\gamma_0 \middle| \begin{matrix} (1,1) \\ (0,1), \theta_1, \cdots, \theta_{N_B} \end{matrix} \right]. \tag{7.38}$$

7.5.2.1 Exact Analysis

Theorem 18. *The secrecy outage probability over cascaded $\alpha-\mu$ wiretap fading channels, in the presence of non-colluding eavesdroppers, is given by (7.39),*

$$\mathscr{P}_{out}(R_s) = 1 - \frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}\mathscr{W}}{\mathscr{C}_{N_B}R_s} \times H_{1,0;N_E,1;N_B,1}^{0,1;1,N_E;0,N_B}\left[\frac{R_s}{\mathscr{C}_{N_E}\mathscr{W}}, \frac{1}{\mathscr{C}_{N_B}\mathscr{W}}\middle|\begin{matrix}(2,1,1)\\ -\end{matrix}\middle|\begin{matrix}\bar{\Theta}_1,\cdots,\bar{\Theta}_{N_E}\\ (1,1)\end{matrix}\middle|\begin{matrix}\bar{\Phi}_1,\cdots,\bar{\Phi}_{N_B}\\ (0,1)\end{matrix}\right], \tag{7.39}$$

where $\bar{\Theta}_j = (1-\mu_{E,j}+\frac{2}{\alpha_{E,j}}, \frac{2}{\alpha_{E,j}})$ *and* $\bar{\Phi}_i = (1-\mu_{B,i}, \frac{2}{\alpha_{B,i}})$.

Proof. See Appendix. III.2. □

Remark 8. The secrecy outage probability over cascaded $\alpha-\mu$ wiretap fading channels is lower bounded by

$$\mathscr{P}_{out}^{L} = 1 - \frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\mathscr{C}_{N_B}\mathscr{C}_{N_E}} H_{N_E+1,N_B+1}^{N_B+1,N_E}\left[\frac{R_s\mathscr{C}_{N_B}}{\mathscr{C}_{N_E}}\middle|\begin{matrix}\bar{\Theta}_1,\cdots,\bar{\Theta}_{N_E},(1,1)\\ (0,1),\Phi_1,\cdots,\Phi_{N_B}\end{matrix}\right]. \tag{7.40}$$

Proof. As $\bar{\gamma}_E$ tends to ∞, it physically means that the eavesdropper is super close to the transmitter, the $\mathscr{P}_{out}$ is lower bounded by

$$\begin{aligned}
\mathscr{P}_{out} &= \mathscr{P}r(\gamma_B \le R_s\gamma_E + \mathscr{W}) \\
&\ge \underbrace{\mathscr{P}r(\gamma_B \le R_s\gamma_E)}_{\mathscr{P}_{out}^{L}} \\
&= 1 - \int_0^\infty \bar{F}_B(R_s\gamma_E) f_E(\gamma_E) d\gamma_E \\
&= 1 - \frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\mathscr{C}_{N_B}} \int_0^\infty H_{0,N_E}^{N_E,0}\left[\mathscr{C}_{N_E}\gamma_E\middle|\begin{matrix}-\\ \Theta_1,\cdots,\Theta_{N_E}\end{matrix}\right] \\
&\qquad \times H_{1,N_B+1}^{N_B+1,0}\left[\mathscr{C}_{N_B}R_s\gamma_E\middle|\begin{matrix}(1,1)\\ (0,1),\Phi_1,\cdots,\Phi_{N_B}\end{matrix}\right] d\gamma_E,
\end{aligned} \tag{7.41}$$

subsequently, the proof is achieved by using the Mellin transform of the product of two Fox's H-function (Prudnikov *et al.*, 1990, eq.(2.25.1.1)). □

Remark 9. When $\alpha_{B,i}=2$, and $\alpha_{E,j}=2$, by using the transformation between Meijer's G-function and Fox's H-function (Prudnikov *et al.*, 1990, eq.(8.3.2.21)), the asymptotic analysis of (7.40) can be further simplified as follows in terms of the Meijer's G-function (Gradshteyn & Ryzhik, 2014, eq. (7.811.1)) [2],

$$\mathscr{P}_{out}^{Asy}=1-\frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\mathscr{C}_{N_B}\mathscr{C}_{N_E}}G_{N_E+1,N_B+1}^{N_B+1,N_E}\left[\frac{R_s\mathscr{C}_{N_B}}{\mathscr{C}_{N_E}}\middle|\begin{matrix}1-\mu_{E,1},\cdots,1-\mu_{E,N_E},1\\0,\mu_{B,1},\cdots,\mu_{B,N_B}\end{matrix}\right]. \tag{7.42}$$

7.5.2.2 Asymptotic Analysis

By using the residue approach given in Chergui *et al.* (2016), the asymptotic behavior of $\mathscr{P}_{out}$ is given in Table. 7.3.

Table 7.3 Asymptotic analysis of the $\mathscr{P}_{out}$

Scenario	**Asymptotic** $\mathscr{P}_{out}$
$\bar{\gamma}_E\to\infty$	$1-\frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\mathscr{C}_{N_B}\mathscr{C}_{N_E}}\left[\frac{\prod_{i=1}^{N_B}\Gamma\left(\mu_{B,i}+\frac{\alpha_{E,k}\mu_{E,k}}{\alpha_{B,i}}\right)\prod_{j=1}^{N_E-1}\Gamma\left(\mu_{E,j}-\frac{\alpha_{E,k}\mu_{E,k}}{\alpha_{E,j}}\right)}{\mu_E}\left(\frac{\mathscr{C}_{N_E}}{\mathscr{C}_{N_B}R_s}\right)^{\frac{\alpha_{E,k}\mu_{E,k}}{2}}\right]$, (7.43) where $\alpha_{E,k}\mu_{E,k}=\min(\alpha_{E,1}\mu_{E,1},\cdots,\alpha_{E,j}\mu_{E,j}), j=1,\cdots,N_E$.
$\bar{\gamma}_B\to\infty$	$\frac{\prod_{j=1}^{N_E}\Gamma\left(\mu_{E,j}+\frac{\alpha_{B,k}\mu_{B,k}}{\alpha_{E,j}}\right)\prod_{i=1}^{N_B-1}\Gamma\left(\mu_{B,i}-\frac{\alpha_{B,k}\mu_{B,k}}{\alpha_{B,i}}\right)}{\mu_{B,k}}\left(\frac{\mathscr{C}_{N_B}R_s}{\mathscr{C}_{N_E}}\right)^{\frac{\alpha_{B,k}\mu_{B,k}}{2}}$, (7.44) where $\alpha_{B,k}\mu_{B,k}=\min(\alpha_{B,1}\mu_{B,1},\cdots,\alpha_{B,i}\mu_{B,i}), i=1,\cdots,N_B$.
$\bar{\gamma}_E\to 0$	$1-\frac{\mathscr{K}_{N_B}}{\mathscr{C}_{N_B}}H_{1,N_B+1}^{N_B+1,0}\left[\frac{R_s\mathscr{C}_{N_B}}{\mathscr{C}_{N_E}}\middle|\begin{matrix}(1,1)\\(0,1),\theta_1,\cdots,\theta_{N_B}\end{matrix}\right]$, (7.45)
$\bar{\gamma}_B\to 0$	1

[2] The implementation of the Meijer's G-function is available in mathematical packages, like Matlab2017b, Maple and Mathematica Mei.

Proof. See Appendix. III.3. □

7.5.3 Probability of Non-zero Secrecy Capacity

Recalling the secrecy capacity over Wyner's wiretap channel, a non-zero secrecy capacity event happens when $\mathscr{C}_s$ is positive on the condition that $\gamma_B > \gamma_E$. By deploying the math language, it can be thus expressed as follows

$$\mathscr{P}_{nz} = Pr(C_s > 0) = Pr(\gamma_B > \gamma_E) = Pr\left(\frac{\gamma_E}{\gamma_B} < 1\right) = F_{\frac{\gamma_E}{\gamma_B}}(1). \tag{7.46}$$

7.5.3.1 Exact Analysis

Theorem 19. *The probability of non-zero secrecy capacity over cascaded $\alpha-\mu$ wiretap fading channels is given by*

$$\mathscr{P}_{nz} = 1 - \frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\mathscr{C}_{N_B}\mathscr{C}_{N_E}} H^{N_E+1,N_B}_{N_B+1,N_E+1}\left[\frac{\mathscr{C}_{N_E}}{\mathscr{C}_{N_B}}\middle|\begin{matrix}\bar{\Phi}_1,\cdots,\bar{\Phi}_{N_B},(1,1)\\ (0,1),\theta_1,\cdots,\theta_{N_E}\end{matrix}\right], \tag{7.47}$$

where $\theta_j = \left(\mu_{E,j}, \frac{2}{\alpha_{E,j}}\right)$.

Proof. Recalling the Remark. 7, and subsequently applying (Bodenschatz, 1992, Eq. (3.7)), the proof is completed. □

Motivated by **Remark** 9, when $\alpha_{B,i} = 2$, and $\alpha_{E,j} = 2$, which means both the main and the wiretap channel undergo the Nakagami-*m* fading, the $\mathscr{P}_{nz}$ is indeed over the cascaded Nakagami-*m* wiretap fading channels, and it is thus given by

$$\mathscr{P}_{nz} = 1 - \frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\mathscr{C}_{N_B}\mathscr{C}_{N_E}} G^{N_E+1,N_B}_{N_B+1,N_E+1}\left[\frac{\mathscr{C}_{N_E}}{\mathscr{C}_{N_B}}\middle|\begin{matrix}1-\mu_{B,1},\cdots,1-\mu_{B,N_B},1\\ 0,\mu_{E,1},\cdots,\mu_{E,N_E}\end{matrix}\right]. \tag{7.48}$$

7.5.3.2 Asymptotic Analysis

When $R_t = 0$, $R_s = 1$, in accordance with the definition of SOP and PNZ, we have

$$\mathscr{P}_{out} = Pr(\gamma_E \leq R_s\gamma_B + R_s - 1) = 1 - \underbrace{Pr(\gamma_B \geq \gamma_E)}_{\mathscr{P}_{nz}}. \tag{7.49}$$

Consequently, the asymptotic behavior of the PNZ can be easily derived by making some simple algebraic substitutions.

7.5.4 Average Secrecy Capacity

Theorem 20. *The average secrecy capacity over cascaded $\alpha-\mu$ wiretap fading channels is given by (7.50),*

$$\begin{aligned}\bar{C}_s = &\underbrace{\frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\ln(2)\mathscr{C}_{N_B}\mathscr{C}_{N_E}} H^{0,N_B;1,2;N_E,1}_{N_B,0;2,2;1,N_E+1}\left[\frac{1}{\mathscr{C}_{N_B}}, \frac{\mathscr{C}_{N_E}}{\mathscr{C}_{N_B}}\middle| \begin{matrix} D_1,\cdots,D_{N_B} \\ - \end{matrix}\middle| \begin{matrix}(1,1),(1,1)\\(1,1),(0,1)\end{matrix}\middle| \begin{matrix}(1,1)\\ \theta_1,\cdots,\theta_{N_E},(0,1)\end{matrix}\right]}_{\mathscr{I}_1} \\ &+\underbrace{\frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\ln(2)\mathscr{C}_{N_B}\mathscr{C}_{N_E}} H^{0,N_E;1,2;N_B,1}_{N_E,0;2,2;1,N_B+1}\left[\frac{1}{\mathscr{C}_{N_E}}, \frac{\mathscr{C}_{N_B}}{\mathscr{C}_{N_E}}\middle| \begin{matrix} E_1,\cdots,E_{N_E} \\ - \end{matrix}\middle| \begin{matrix}(1,1),(1,1)\\(1,1),(0,1)\end{matrix}\middle| \begin{matrix}(1,1)\\ \phi_1,\cdots,\phi_{N_B},(1,1)\end{matrix}\right]}_{\mathscr{I}_2} \\ &+\underbrace{\frac{\mathscr{K}_{N_E}}{\ln(2)\mathscr{C}_{N_E}} H^{1,2+N_E}_{2+N_E,2}\left[\frac{1}{\mathscr{C}_{N_E}}\middle| \begin{matrix}(1,1),(1,1),\left(1-\mu_{E,l},\frac{2}{\alpha_{E,l}}\right),\cdots,\left(1-\mu_{E,N_E},\frac{2}{\alpha_{E,N_E}}\right)\\(1,1),(0,1)\end{matrix}\right]}_{\mathscr{I}_3},\end{aligned} \tag{7.50}$$

where $D_i = \left(1-\mu_{B,i},\frac{2}{\alpha_{B,i}},\frac{2}{\alpha_{B,i}}\right)$, $E_j = \left(1-\mu_{E,j},\frac{2}{\alpha_{E,j}},\frac{2}{\alpha_{E,j}}\right)$, $\phi_i = \left(\mu_{B,i},\frac{2}{\alpha_{B,i}}\right)$, $H^{m,n;m_1,n_1;m_2;n_2}_{p,q;p_1,q_1;p_2,q_2}[.]$ and $H^{m,n}_{p,q}[.]$ are the bivariate and univariate Fox's H-function (Mathai et al.*, 2009a, Eqs. (1.2) and (2.56)), respectively.*

Proof. See Appendix. III.4. □

7.6 Numerical Results and Discussions

In this section, we confirm the accuracy of our analytical derivations demonstrated in Sections 7.4 and 7.5, in comparison with Monte-Carlo simulation results[3]. For the conciseness of illustrations, the curves only with markers are the Monte-Carlo simulation outcomes, whereas the ones denoted with lines are used to depict our analytical results.

7.6.1 Reliability Analysis over Cascaded α-μ Fading Channels

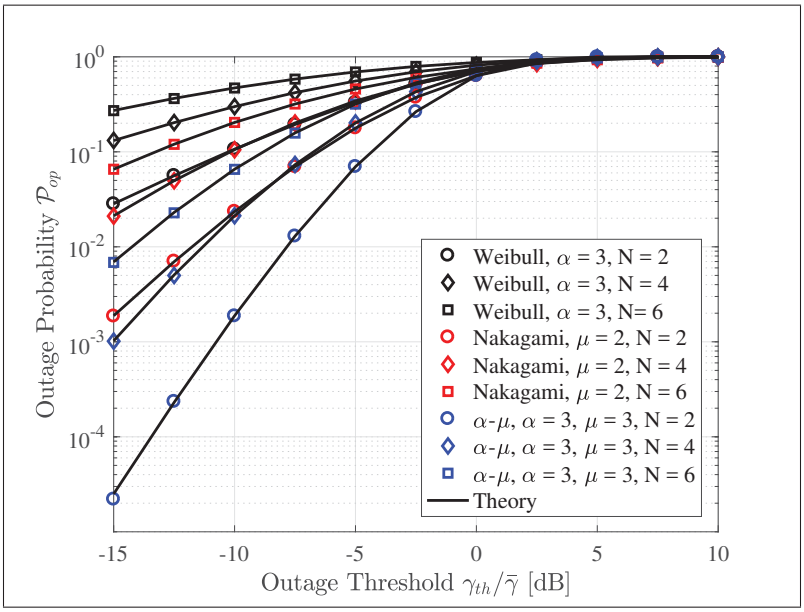


Figure 7.4 $\mathscr{P}_{op}$ versus $\gamma_{th}/\bar{\gamma}$ over cascaded $\alpha-\mu$ wiretap fading channels for selected values of N

Considering the system configuration shown in Fig. 7.1, in Figs. 7.4-7.6, we plot the outage probability, the average channel capacity and the ASEP with coherent demodulation scheme over cascaded $\alpha-\mu$ fading channels, respectively.

[3] It is worthy to mention that (i) the $\alpha-\mu$ fading channel is implemented by using the WAFO toolboxBrodtkorb *et al.* (2000); (ii) the implementation of the Fox's H-function is computationally practicable, the numerical evaluation of univariate and bivariate Fox's H-function of (7.39) and (7.40) for MATLAB implementations are based on the method proposed in (Peppas *et al.*, 2012, Table. II) and (Peppas, 2012, Appendix. A), respectively.

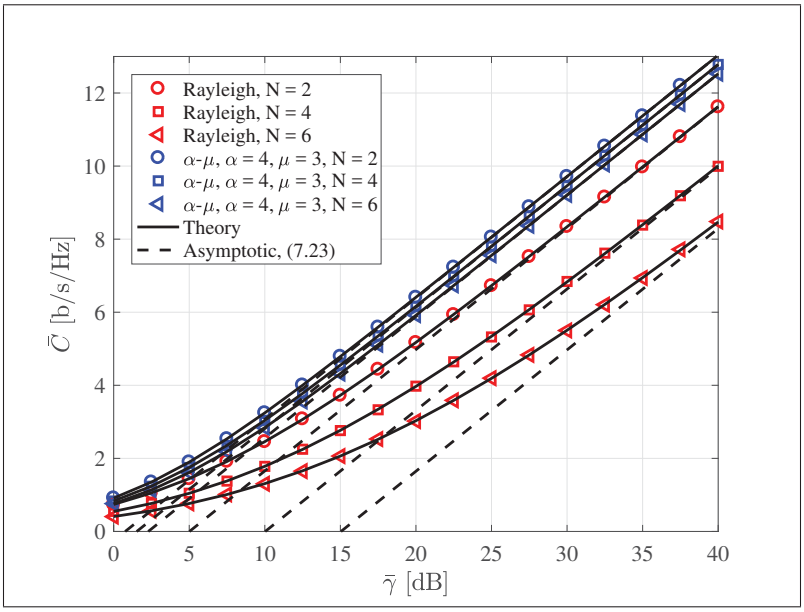


Figure 7.5 Average channel capacity $\bar{C}$ over cascaded $\alpha - \mu$ fading channels

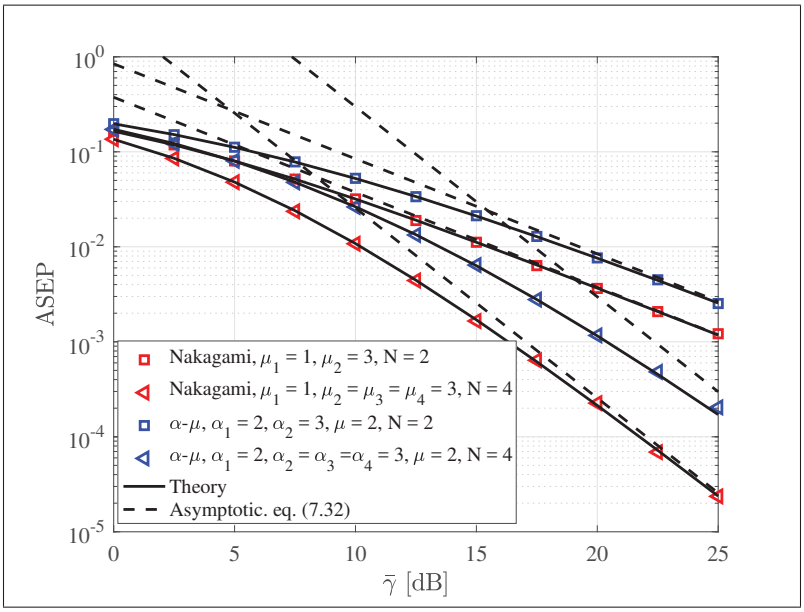


Figure 7.6 The ASEP $\bar{\mathscr{P}}_{se}^{C}$ over cascaded $\alpha - \mu$ fading channels

Those figures reveal that our derivations given by (7.16), (7.19) and (7.25) are in perfect match with simulation outcomes, which are particularly validated for several specific cases, such as Rayleigh, Nakagami-m, and Weibull, respectively.

To terminate the reliability analysis over cascaded $\alpha-\mu$ fading channels, one can perceive the following conclusions from the three figures (i) the performance metrics physically demonstrate worse trend with the increase of N, outstandingly, it is caused by the fact that the multiplication of several successive fading makes it less likely to transmit the desired messages successfully; (ii) for a given fading scenario, reliable communication can be assured only by increasing the transmitting power.

7.6.2 Secrecy Analysis over Cascaded α-μ Wiretap Fading Channels

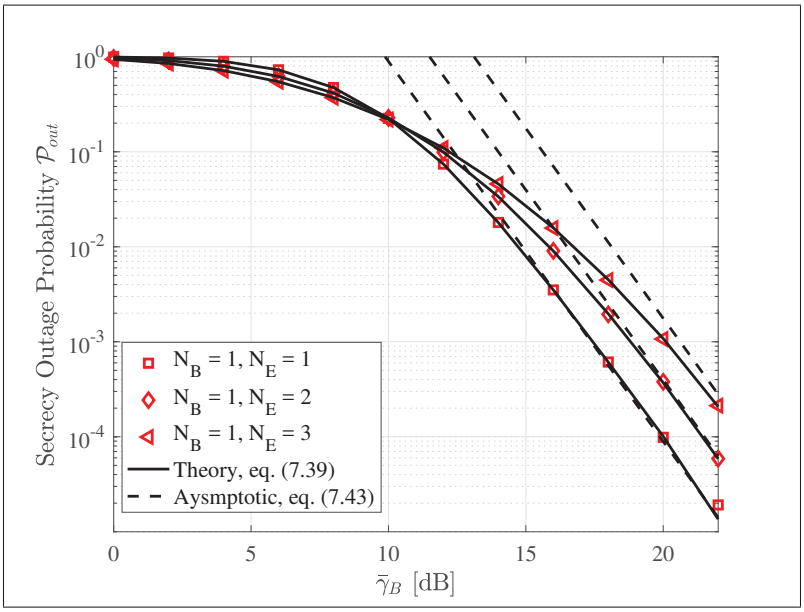


Figure 7.7 $\mathscr{P}_{out}$ versus $\bar{\gamma}_B$ over cascaded $\alpha-\mu$ wiretap fading channels when $\bar{\gamma}_E$ = 6 dB, $R_s = 0.5$, $\alpha_B = 4$, $\mu_B = 2$, $\alpha_E = 2$, and $\mu_E = 3$

In the presence of a malicious eavesdropper, the secrecy outage probability and probability of non-zero secrecy capacity are presented in this subsection. Fig. 7.7 plots the secrecy outage probability $\mathscr{P}_{out}$ against the average transmitted power $\bar{\gamma}_B$ when fixing N_B and N_E for selected

values. From this figure, it is observed that $\mathscr{P}_{out}$ decreases with the increase of $\bar{\gamma}_B$, which is due to a better secrecy capacity which can be achieved with the increase of $\bar{\gamma}_B$. In addition, the secrecy outage probability is, as expected, strongly influenced by the value of N_B and N_E, namely, the number of relays or keyholes. Naturally, this phenomenon can be explained via the fact that more keyholes mean much severer propagation on the legitimate signals.

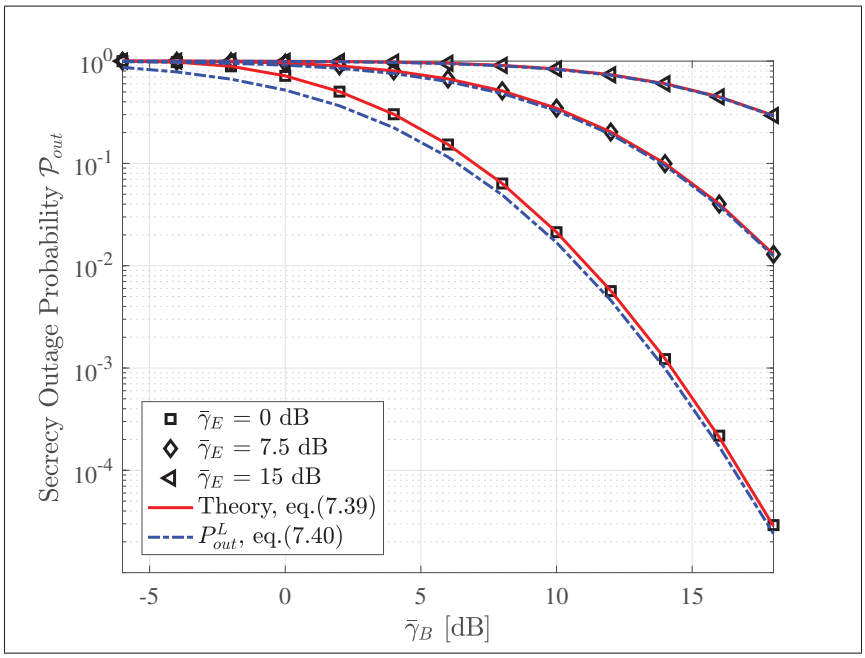


Figure 7.8 $\mathscr{P}_{out}$ versus $\bar{\gamma}_B$ over cascaded $\alpha-\mu$ wiretap fading channels when $N_B = N_E = 2$, $R_s = 0.5$, $\alpha_B = 4$, $\mu_B = 3$, $\alpha_E = 2$, and $\mu_E = 2$

Additionally, as shown in Fig. 7.8, our derived asymptotic expression, the $\mathscr{P}^{Asy}_{out}$ given in (7.40), closely approximates the exact secrecy outage probability $\mathscr{P}_{out}$, in particular, the gap between them is becoming smaller as $\bar{\gamma}_E$ increases.

In Fig. 7.9, we compare our analytical $\mathscr{P}_{nz}$ given in (7.47) with Monte-Carlo simulation results. On the contrary with $\mathscr{P}_{out}$, positive secrecy capacity can be surely guaranteed with a higher probability as $\bar{\gamma}_B$ increases.

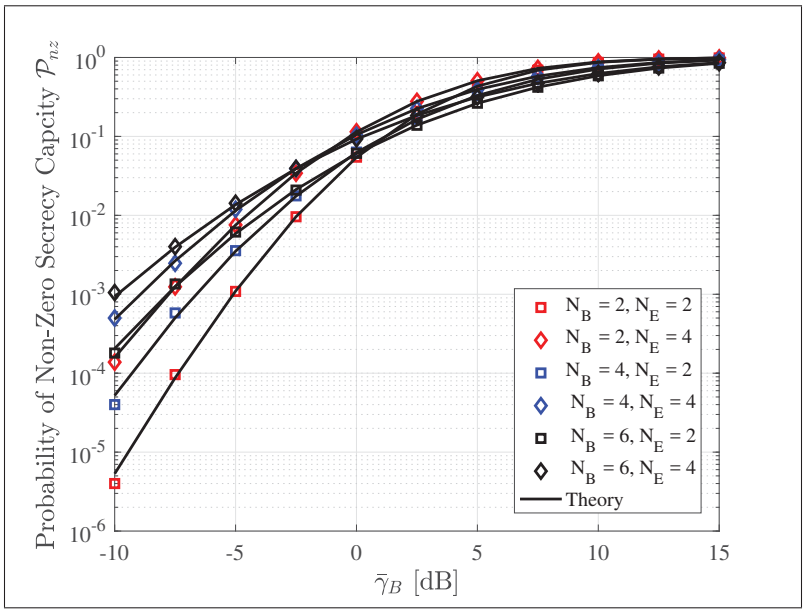


Figure 7.9 $\mathscr{P}_{nz}$ versus $\bar{\gamma}_B$ over cascaded $\alpha-\mu$ wiretap fading channels when $\bar{\gamma}_E$ = 5 dB, $\alpha_B = 3$, $\mu_B = 2$, $\alpha_E = 2$, and $\mu_E = 2$

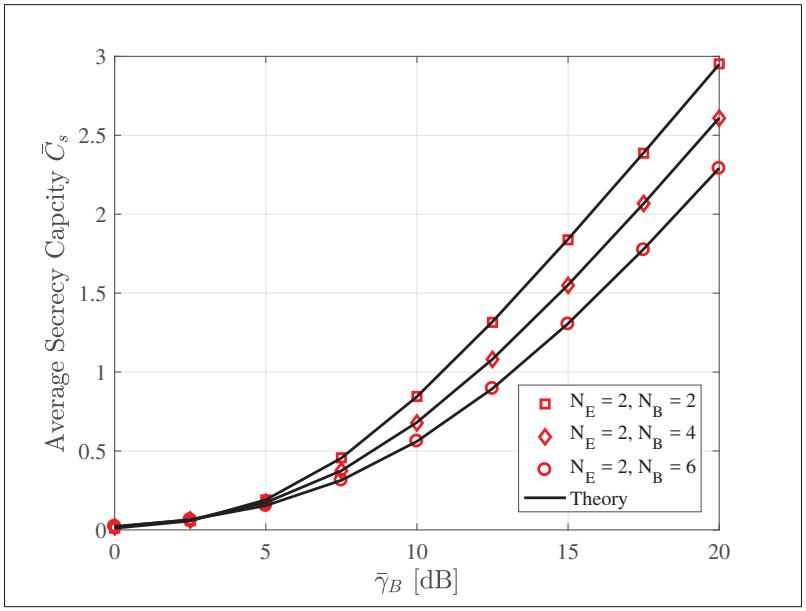


Figure 7.10 $\bar{C}_s$ versus $\bar{\gamma}_B$ for selected N_B when $\alpha_B = 3$, $\alpha_E = 4$, $\mu_B = 2$, $\mu_E = 3$, and $\bar{\gamma}_E = 5$dB

In Figs. 7.10-7.11, the average secrecy capacity against $\bar{\gamma}_B$ is presented for three case: (i) selected values of N_B; (ii) selected values of N_E; An obvious conclusion can be summarized from Figs. 7.10 and 7.11 that: the average secrecy capacity is improved with the increase of N_E and degraded with the increase of N_B. This is due to the fact, i.e., the bigger N_B (or N_E), the worse quality of the received SNR of Bob (or Eve).

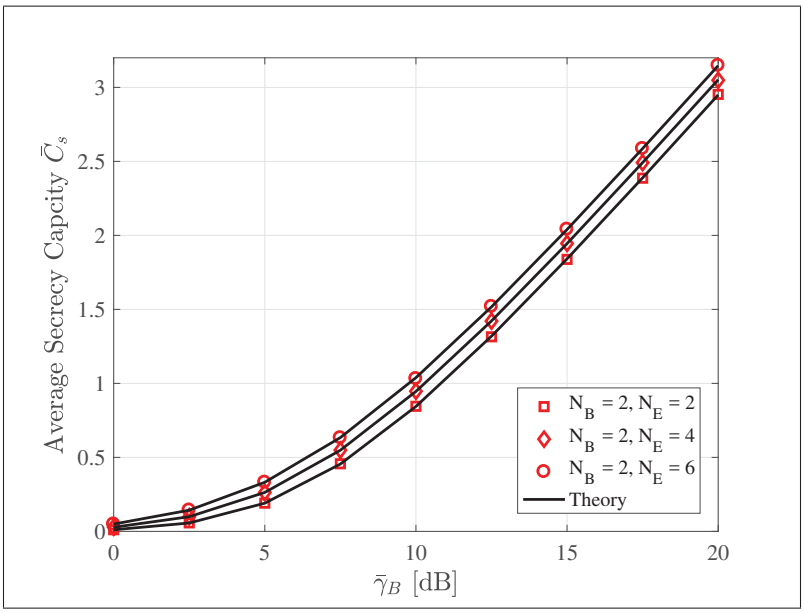


Figure 7.11 $\bar{C}_s$ versus $\bar{\gamma}_B$ for selected N_E when $\alpha_B = 3$, $\alpha_E = 4$, $\mu_B = 2$, $\mu_E = 3$, and $\bar{\gamma}_E = 5$dB

Overall, interesting observations drawn from Figs. 7.7 and 7.9 can be summarized as follows (i) our analytical results given by (7.39) and (7.47) are successfully verified by Monte-Carlo simulation outcomes; (ii) no matter for the $\mathscr{P}_{out}$ or $\mathscr{P}_{nz}$, the number of keyholes or relays is of great significance with the system security performance.

7.7 Conclusion and Future Work

In this paper, the notion of $N*(\alpha-\mu)$ cascaded fading channels was introduced, together with its statistics characteristics. As stated in the context, it can be respectively reduced to the

cascaded Rayleigh, Weibull, Nakagami-m fading channels by attributing α and μ to specific values.

Based on such a general channel model, we further investigated one wireless multi-hop AF relaying link when considering two scenarios: in the absence and presence of a malicious eavesdropper. Regarding the former scenario, the outage probability, average channel capacity and the ASEP were deduced with closed-form expressions, which were derived in terms of the Fox's H-function. When it comes to the latter case, we studied such a digital communication system from the information theoretical perspective. The secrecy metrics, including the secrecy outage probability, the probability of non-zero secrecy capacity, and average secrecy capacity were evaluated, which were correspondingly given with respect to the bivariate and univariate Fox's H-function. In addition, the asymptotic analysis of the secrecy outage probability was also derived and therefore compared with the exact expression. Subsequently, our analytical mathematical representations for both cases were further successfully verified via the Monte-Carlo simulation outcomes.

As readily observed from our work, it is so far limited to the investigations of digital wireless communication systems under the assumptions of independent $N*(\alpha-\mu)$ fading channels, generally speaking, one possible future research direction may be the extension of our results to the correlated cascaded $N*(\alpha-\mu)$ fading channels.

CHAPTER 8

SECRECY ANALYSIS OF RANDOM MIMO WIRELESS NETWORKS OVER $\alpha - \mu$ FADING CHANNELS

Long Kong[1], Satyanarayana Vuppala[2], and Georges Kaddoum[1]

[1]Département de Génie électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3
[2]United Technologies Research Center, Cork, Ireland

Paper published in *IEEE Transactions on Vehicular Technology*, December. 2018.

8.1 Abstract

In this paper, we investigate the secrecy performance of stochastic MIMO wireless networks over small-scale $\alpha - \mu$ fading channels, where both the legitimate receivers and eavesdroppers are distributed with two independent homogeneous Poisson point processes (HPPPs). Specifically, accounting for the presence of non-colluding eavesdroppers, secrecy performance metrics, including the connection outage probability (COP), the probability of non-zero secrecy capacity (PNZ) and ergodic secrecy capacity, are derived regarding the k-th nearest/best user cases. The index for the k-th nearest user is extracted from the ordering, in terms of the distances between transmitters and receivers, whereas that for the k-th best user is based on the combined effects of path-loss and small-scale fading. In particular, the probability density functions (PDFs) and cumulative distribution functions (CDFs) of the composite channel gain, for the k-th nearest and best user, are characterized, respectively. Benefiting from these results, closed-form representations of the COP, PNZ and ergodic secrecy capacity are subsequently obtained. Furthermore, a limit on the maximal number of the best-ordered users is also computed, for a given secrecy outage constraint. Finally, numerical results are provided to verify the correctness of our derivations. Additionally, the effects of fading parameters, path-loss exponent, and density ratios are also analyzed.

Keywords: Physical layer security, Poisson point process, $\alpha - \mu$ fading, random MIMO wireless networks, *k*-th legitimate user.

8.2 Introduction

The security issue impacting the wireless networks has recently attracted significant attention from the academic and industrial communities. In this vein, the development of conventional approaches, based on cryptography techniques, faces new challenges, especially in large-scale wireless network, due to its high power consumption and complexity requirements. Alternatively, physical layer security (PLS) appears as an appealing strategy to address such a concern by conversely exploiting the inherent randomness and noisy characteristics of radio channels in order to protect confidential messages from being wiretapped.

8.2.1 Background and Related Works

The fundamental of the PLS was initially built on the discovery of '*perfect secrecy*' by Shannon Shannon (1949) and the conceptual finding of degraded 'wiretap channel', for the discrete memoryless channel, by Wyner Wyner (1975). Later on, successive efforts were devoted to the generalization of the results in Wyner (1975) to additive Gaussian noise channels Leung-Yan-Cheong & Hellman (1978), broadcast channels Csiszar & Korner (1978), fading channels Bloch *et al.* (2008); Gopala *et al.* (2008); Kong *et al.* (2016b); Lei *et al.* (2015,1), multiple-input multiple-output (MIMO) communications Chen, X. & Yin, R. (2013); Kong *et al.* (2016a); Zhu, J., Zou, Y., Wang, G., Yao, Y. D. & Karagiannidis, G. K. (2016), cooperative networks Thai, C. D. T., Lee, J. & Quek, T. Q. S. (2016), cellular networks Tolossa *et al.* (2018); Vuppala *et al.* (2018) among other topics.

A common shortage of the aforesaid works Bloch *et al.* (2008); Csiszar & Korner (1978); Gopala *et al.* (2008); Kong *et al.* (2016a,1); Lei *et al.* (2015,1); Leung-Yan-Cheong & Hellman (1978); Thai *et al.* (2016), based on the point-to-point communication links, lies in the uncertainty of users' spatial locations. Strictly speaking, users' spatial locations undoubtedly

play a crucial role when investigating the large scale fading in random networks. The pioneer works, led by Haenggi Haenggi, M. (2008a,0), and where users distributed randomly based on stochastic geometry, was modeled as the Poisson point process (PPP). Specifically, it is worthy to mention that the concept of 'secrecy graph' was firstly proposed to study the secrecy connectivity metric, and subsequently the maximum secrecy rate Pinto, P. C., Barros, J. & Win, M. Z. (2012b) when colluding eavesdroppers are considered.

More recently, in Bai, J., Tao, X., Xu, J. & Cui, Q. (2014); Jeong, Y., Quek, T. Q. S., Kwak, J. S. & Shin, H. (2014); Liu *et al.* (2014); Tolossa, Y. J., Vuppala, S. & Abreu, G. (2017); Zheng, T. X., Wang, H. M. & Yin, Q. (2014), the authors considered the two-dimensional random wireless network under Rayleigh, composite fading and Nakagami-*m* fading channels, where both the legitimate receivers and eavesdroppers are drawn from two independent homogeneous PPPs (HPPPs). Authors in Jeong *et al.* (2014) studied the secure MIMO transmission subjected to Rayleigh fading. Zheng *et al.* in Zheng *et al.* (2014) analyzed the transmission secrecy outage probability for multiple-input and single-output (MISO) systems, and proposed the concept of '*security region* (SR)', which is a geometry region, defined as the legitimate receiver's locations having a certain guaranteed level of secrecy. Differently, Satyanarayana *et al.* proposed another SR[1] Vuppala, S., Biswas, S., Ratnarajah, T. & Sellathurai, M.; Vuppala, S., Biswas, S. & Ratnarajah, T. (2017), which is defined as the region where the set of ordered nodes can safely communicate with typical destination, for a given secrecy outage constraint.

Motivated by those references, it is thus of tremendous significance to study how many legitimate users are located within the coverage of the transmitter (i.e., base station), in the presence of unknown number of eavesdroppers. Most of the existing work can be summarized in terms of the ordering policy, namely the *k*-th legitimate user, either based on the distances between transmitters and users, or the instantaneous received composite channel gain. Moving in this direction, it is reported that limited studies are seen on the secrecy assessment of the *k*-th legitimate receiver. Specifically, the result disclosed in Bai *et al.* (2014) is merely restricted to the mathematical treatment of the secrecy outage probability of the *k*-th nearest receiver (i.e., the

[1] Within the security region, all users can achieve high secrecy gains.

index is from the ordering based on the distance between the source and the destination). In contrast, the results unveiled in Liu *et al.* (2014); Tolossa *et al.* (2017); Vuppala *et al.*, 2017) are constrained to the k-th best receiver[2] (i.e., the index is according to the array of the composite channel gains). It is reported that Chen, G. & Coon, J. P. (2017) investigated the secrecy issue over Rayleigh fading channels, while considering both ordering policies without offering any SR. On the other hand, the introduced k-th nearest or best receiver is applicable to vehicular networks. The k-th best user can be considered as any potential vehicle receiving the *k-th maximum path gain* from a source vehicle. One can construct the security region by selecting all the best nodes instead of random users. Selecting the best users to coordinate among each other can further improve the security of the network.

Outstandingly, the aforesaid studies merely focus on the secrecy analysis, influenced by the colluding/non-colluding eavesdroppers but have not taken the more general fading model, namely, $\alpha - \mu$ fading channel, into consideration. The $\alpha - \mu$ distribution was first proposed by Yacoub in Yacoub (2007a) to model the small scale variation of fading signal under line-of-sight conditions Leonardo & Yacoub (2015b); Papazafeiropoulos, A. K. & Kotsopoulos, S. A. (2010). It is physically described with two key fading parameters, i.e., non-linearity of the propagation medium α and the clustering of the multipath waves μ. The advantage of these two factors is regarded as a useful tool to vividly depict the inhomogeneous surroundings compared with other existing fading models, such as Rayleigh, Nakagami-m. Most of them are based on the unrealistic assumption of homogeneous (scattering) environment. Fortunately, the $\alpha - \mu$ fading model was later on found valid and feasible in many realistic situations Chong *et al.* (2011); Dias & Yacoub (2009); Karadimas *et al.* (2010); Michalopoulou *et al.* (2011,1); Reig & Rubio (2013); Wu *et al.* (2010), including the vehicle-to-vehicle (V2V) communication networks and wireless body area networks (WBAN). In addition, the $\alpha - \mu$ distribution is flexible and mathematical tractable, since it can be extended to Rayleigh, Nakagami-m and Weibull fading by simply attributing the fading parameters α and μ to selected values. For

[2] It is worth mentioning that the k-th best user is the one with the k-th maximal received signal out of K users.

example, choosing $\alpha = 2$ and $\mu = 1$ will reduce it to Rayleigh fading, while choosing $\alpha = 2$ and $\mu = m$ will make it correspond to Nakagami-*m* fading.

To the best knowledge of the authors, in Kong *et al.* (2016b); Lei *et al.* (2015), the authors derived the probability of non-zero secrecy capacity and secrecy outage probability of point-to-point communication over $\alpha - \mu$ fading channels. Lei *et al.* Lei *et al.* (2017a) later on studied the average secrecy capacity of $\alpha - \mu$ wiretap fading channels. The importance of evaluating the aforementioned two metrics is based on the behavior of the eavesdroppers. If they are active, meaning that it is possible to have their channel state information (CSI) at the transmitter, the probability of non-zero secrecy capacity and the secrecy outage probability are crucial. If they are passive, average secrecy capacity is therefore a key benchmark. With respect to the random single-input and single-output (SISO) wireless networks, the authors in Vuppala *et al.*, 2017) and Liu, W., Ding, Z., Ratnarajah, T. & Xue, J. (2016) correspondingly investigated the secrecy outage probability and the ergodic secrecy capacity in terms of the *k*-th best user, respectively. Apart from the literature Kong *et al.* (2016b,1,1); Lei *et al.* (2015,1); Liu *et al.* (2016); Vuppala *et al.*, 2017), efforts to explore the secrecy evaluation of random MIMO wireless networks over $\alpha - \mu$ fading channels are rarely witnessed.

8.2.2 Contribution and Organization

Consequently, the essence of this paper is the exploration of the *k*-th legitimate user's secrecy performance over $\alpha - \mu$ fading channel in typical random wireless networks.

In this paper, we consider a stochastic MIMO wireless system, in the presence of two types of receivers, namely, legitimate users and eavesdroppers. They are assumed to be distributed with two independent HPPPs. The conventional space-time transmission (STT) is considered Zhu *et al.* (2016). All receivers have access to perfect channel state information (CSI), which are all subjected to quasi-static $\alpha - \mu$ fading. Since Wyner had concluded that perfect secrecy can be assured only if legitimate links have higher transmission rate, compared to wiretap links, the pursuit of outage-based secrecy performance analysis is considered reasonable and feasible

when a fixed data transmission scheme is adopted for such quasi-static fading channels, as indicated in Tolossa *et al.* (2017); Wang & Wang (2016). In Liu *et al.* (2016), the secure connection probability of the k-th legitimate receiver to the transmitter was studied, as well as the ergodic secrecy capacity.

To this end, the connection outage probability (COP), the probability of non-zero secrecy capacity (PNZ) and the ergodic secrecy capacity, in terms of the k-th nearest and best legitimate receivers, are taken into consideration.

Since the concept of the k-th best user can be regarded as a security region, it is crucial to identify the k^* best users out of K users that can communicate securely with the transmitter in such region. In this work, we identify a zone (i.e., a limited number of legitimate users) comprising of such ordered k^* best users, for a given secrecy constraint.

The contributions of this paper are multifold, which can be pointed out as:

1) The probability of density functions (PDFs) and cumulative distribution function (CDFs) of the composite channel gain for the k-th nearest and best user are derived, respectively. This is essentially important for formulating the secrecy metrics, including the connection outage probability, the probability of non-zero secrecy capacity and ergodic secrecy capacity.

2) Unlike the model studied in Lei *et al.* (2017a), which considered the point-to-point system and a single eavesdropper, we study the secrecy capacity of random networks with multiple legitimate receivers and eavesdroppers. The exact closed form expressions of the COP, PNZ and ergodic secrecy capacity of the k-th legitimate user are derived.

3) Motivated by the PNZ of the k-th best receiver, a limit on the maximal number of the best-ordered receivers is calculated thereafter respecting a given secrecy outage probability. In other words, this limit eventually provides a security region concept, henceforth, all the system parameters are looked upon, based on this concept, giving a better insight into the secrecy capacity regions of random wireless networks.

4) The accuracy of our derivations are successfully validated by Monte-Carlo simulation. Numerical outcomes are presented to indicate the effect of the path-loss exponent, densities of the users and fading parameters.

The insights obtained from the outcomes of this paper, regarding the crucial parameters of the secrecy performance, inspire researchers and vehicle wireless communication engineers to quickly evaluate system performance and optimize available parameters when confronting various security risks.

The rest of this paper is organized as follows: system model and problem formulation are depicted in Sections 8.3 and 8.4, respectively. The COP, PNZ and the ergodic secrecy capacity are derived in Section 8.5. Numerical results and discussions are then presented in Section 8.6 and followed by Section 8.7 with concluding remarks. Notations and symbols used in this paper are shown in Table. 8.1.

8.3 System Model

In this paper, a random wireless network, displayed in Fig. 8.1 in an unbound Euclidean space of dimension d is under consideration. The typical transmitter is located at the origin, who has N_a ($N_a \geq 1$) antennas, and two types of receivers, namely the legitimate receivers and eavesdroppers with N_b ($N_b \geq 1$), N_e ($N_e \geq 1$) antennas, respectively. The locations of these receivers are drawn from two independent HPPPs. Their location sets are separately denoted by $\Phi_b(\lambda_b)$ and $\Phi_e(\lambda_e)$ with corresponding densities λ_b and λ_e Jeong *et al.* (2014); Liu *et al.* (2014). In such a network configuration, it is assumed that the communication links undergo a path-loss characterized by the exponent υ and $\alpha - \mu$ fading.

Consider a transmitter that intends to send private messages to a legitimate user in the presence of eavesdroppers located at some unknown distances r_e. In such a stochastic MIMO wireless system, the conventional STT scheme is considered at the transmitter and receivers Zhu *et al.* (2016), then the instantaneous received signal-to-noise ratios (SNRs) at a legitimate user, γ_b,

Table 8.1 Notations and symbols

Notations	Description
$[x]^+$	$[x]^+ = \max(x, 0)$
$\mathbb{N}$	positive integer
$\mathbb{E}$	expectation operator
i.i.d	identical independent distributed
R_t	transmission rate
d	dimensions of the network
r	distance from the origin to the receiver
υ	path-loss exponent
f_X	PDF of X
F_X	CDF of X
c_d	$\pi^{d/2}/\Gamma(1+d/2)$
δ	d/υ
Ψ	path-loss process before fading
Ξ_k	path-loss process with fading for legitimate users
Ξ_e	path-loss process with fading for eavesdroppers
λ_b	density for legitimate receivers
λ_e	density for eavesdroppers
$\Gamma(a)$	$\Gamma(a) = \int_0^\infty t^{a-1}e^{-t}dt$ Gamma function (Gradshteyn & Ryzhik, 2014, eq. (8.310.1))
$\gamma(a,x)$	$\gamma(a,x) = \int_0^x t^{a-1}e^{-t}dt$ lower incomplete gamma function (Gradshteyn & Ryzhik, 2014, eq. (8.350.1))
$\Gamma(a,x)$	$\Gamma(a,x) = \int_x^\infty t^{a-1}e^{-t}dt$ upper incomplete gamma function(Gradshteyn & Ryzhik, 2014, eq. (8.350.2))
$H_{m,n}^{p,q}[\cdot]$	Fox's H-function (Mathai & Saxena, 1978, eq. (1.1.1))

and an eavesdropper, γ_e, would be expressed as (Zhu *et al.*, 2016, eq.(1))

$$\gamma_b = \frac{P \sum_{n_a=1}^{N_a} \sum_{n_k=1}^{N_b} g_{n_a,n_k}}{r_l^{\upsilon} \sigma_k^2} = \eta_k \frac{g_k}{r_l^{\upsilon}}, \tag{8.1a}$$

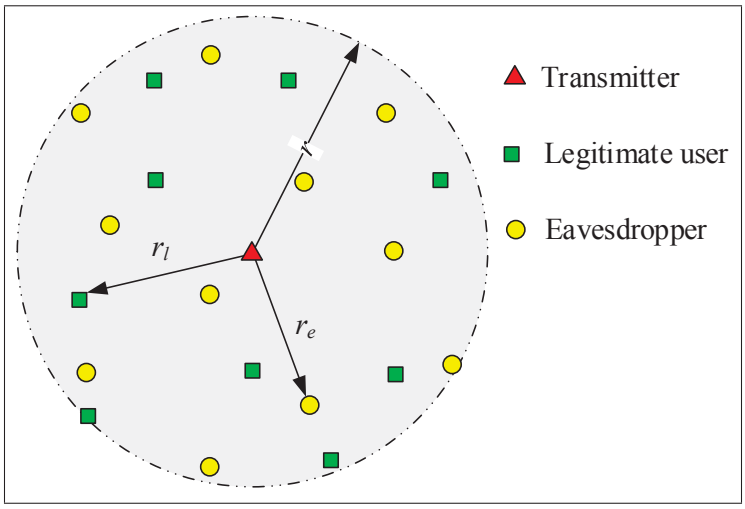


Figure 8.1 A 2-dimensional stochastic MIMO wireless network with independently HPPP distributed legitimate receivers and eavesdroppers

$$\gamma_e = \frac{P \sum_{n_a=1}^{N_a} \sum_{n_e=1}^{N_e} g_{n_a,n_e}}{r_e^{\upsilon} \sigma_e^2} = \eta_e \frac{g_e}{r_e^{\upsilon}}, \tag{8.1b}$$

where $\eta_i = \frac{P}{\sigma_i^2}$, $g_{n_a,n_i} = |h_{n_a,n_i}|^2, i \in \{k,e\}$, denote the instantaneous channel power gain with unit mean. P denotes the transmission power and the terms σ_i denote the noise power at the legitimate and eavesdropping receivers, respectively. So herein, r_l and h_{n_a,n_k} are the distance and fading envelope from the transmitter to the k-th legitimate receiver, respectively. Similarly, r_e and h_{n_a,n_e} are the distance and fading envelope from the transmitter to the eavesdropper, respectively. Here, h_{n_a,n_i} are modeled by $\alpha - \mu$ fading with an arbitrary fading parameter $\alpha_i > 0$ and an inverse normalized variance of $h_i^{\alpha_i}$ denoted as μ_i.

Since STT scheme is used, g_i is obviously the sum of all the receivers' channel gain. Recalling the results obtained in da Costa *et al.* (2008), the exact PDF and CDF of g_i are too complex due to the convolution of M PDFs of each eavesdropper's channel gain when developing the secrecy performance. Thanks to the highly tight approximation method provided therein, it is

deduced therein that the PDF of g_i is given as the following form with parameters (α_i, μ_i, Ω_i)[3],

$$f_{g_i}(x) \approx \frac{\alpha_i x^{\frac{\alpha_i\mu_i}{2}-1}}{2\Omega_i^{\frac{\alpha_i\mu_i}{2}}\Gamma(\mu_i)} \exp\left(-\left(\frac{x}{\Omega_i}\right)^{\frac{\alpha_i}{2}}\right) = \varepsilon_i H_{0,1}^{1,0}\left[\theta_i x \,\middle|\, \begin{matrix} - \\ (\mu_i - \frac{2}{\alpha_i}, \frac{2}{\alpha_i}) \end{matrix}\right], \tag{8.2}$$

where $\Omega_i = \frac{\Gamma(\mu_i)}{\Gamma\left(\mu_i+\frac{2}{\alpha_i}\right)}$, $\varepsilon_i = \frac{1}{\Omega_i\Gamma(\mu_i)}$, and $\theta_i = \frac{1}{\Omega_i}$. After integrating (8.2), the CDF of g_i is given by

$$F_{g_i}(x) = \frac{\gamma\left(\mu_i, \left(\frac{x}{\Omega_i}\right)^{\frac{\alpha_i}{2}}\right)}{\Gamma(\mu_i)} = 1 - \frac{\varepsilon_i}{\theta_i} H_{1,2}^{2,0}\left[\theta_i x \,\middle|\, \begin{matrix} (1,1) \\ (0,1), (\mu_i, \frac{2}{\alpha_i}) \end{matrix}\right]. \tag{8.3}$$

8.4 Problem Formulation

8.4.1 User Association

8.4.1.1 The nearest user

In this case, all the receivers are ordered according to their distance from the transmitter. Let $\{r_k\}$ be a random set of legitimate receivers in ascending order of the distances from the receiver to the transmitter (i.e., $|r_1| < |r_2| < |r_3| < \cdots$). Letting $Z = \frac{g_k}{r_k^{\upsilon}}$, the PDF and CDF of the composite channel gain are respectively given in the following **Lemma**.

Lemma 1. *The PDF and CDF of the composite channel gain for the k-th nearest legitimate user are given by (8.4a) and (8.4b) in terms of the Fox's H-function*[4]*, respectively.*

$$f_{\frac{g_k}{r_k^{\upsilon}}}(z) = \frac{\varepsilon_k}{A_k^{\frac{1}{\delta}}\Gamma(k)} H_{1,1}^{1,1}\left[\frac{\theta_k z}{A_k^{\frac{1}{\delta}}} \,\middle|\, \begin{matrix} (1-k-\frac{1}{\delta}, \frac{1}{\delta}) \\ (\mu_k - \frac{2}{\alpha_k}, \frac{2}{\alpha_k}) \end{matrix}\right], \tag{8.4a}$$

[3] The method of obtaining all these three parameters is suggested to refer to da Costa *et al.* (2008).

[4] The numerical evaluation of Fox's H-function for MATLAB implementations is to use the method given in (Peppas *et al.*, 2012, Table. II).

$$F_{\frac{g_k}{r_k^{\upsilon}}}(z) = 1 - \frac{\varepsilon_k}{\theta_k \Gamma(k)} H_{2,2}^{2,1}\left[\frac{\theta_k z}{A_k^{\frac{1}{\delta}}} \middle| \begin{matrix}(1-k,\frac{1}{\delta}),(1,1)\\(0,1),(\mu_k,\frac{2}{\alpha_k})\end{matrix}\right], \tag{8.4b}$$

where $A_k = \pi\lambda_b$.

Proof. See Appendixes IV.1 and IV.2, respectively. □

Similarly, the PDF and CDF for the k-th nearest eavesdropper can be obtained with parameters $A_e = \pi\lambda_e$.

8.4.1.2 The best user

Unlike the nearest user, the k-th best user describes the ordering of the recerivers according to the received SNR function of the combination of the path-loss and small-scale fading. Letting $\Xi_k = \{\xi_k \triangleq r_k^{\upsilon}/g_k, k \in \mathbb{N}\}$ be the path-loss process with small-scale fading. It is reported in Haenggi (2008b) that Ξ_k is also a PPP with the intensity function λ_{Ξ_k}. For the k-th best user, we have $|\xi_1| < |\xi_2| < |\xi_3| < \cdots$, since ξ_k takes the inverse shape of the composite channel gain.

Lemma 2. *Given the path-loss process with the* $\alpha-\mu$ *fading, the intensity of* Ξ_k *is given by*

$$\lambda_{\Xi_k} = A_{b0} x^{\delta-1}, \tag{8.5}$$

where $A_{b0} = \frac{\lambda_b c_d \delta \Omega_k^{\delta} \Gamma\left(\mu_k + \frac{2\delta}{\alpha_k}\right)}{\Gamma(\mu_k)}$.

Proof. See Appendix IV.3. □

Similarly, with regard to eavesdroppers, we have $\Xi_e = \{r_e^{\upsilon}/g_e, e \in \mathbb{N}\}$, $\lambda_{\Xi_e} = A_{e0} y^{\delta-1}$, $A_{e0} = \frac{\lambda_e c_d \delta \Omega_e^{\delta} \Gamma\left(\mu_e + \frac{2\delta}{\alpha_e}\right)}{\Gamma(\mu_e)}$.

Let $\frac{1}{\xi_k} = Z$, then the PDF and CDF of $\frac{1}{\xi_k}$ are provided in the following Lemma.

Lemma 3. *The PDF and CDF of the composite channel gain for the k-th best user are*

$$f_{\frac{1}{\xi_k}}(z) = \exp\left(-A_{b1}z^{-\delta}\right)\frac{\delta(A_{b1}z^{-\delta})^k}{z^{-1}\Gamma(k)}. \tag{8.6a}$$

$$F_{\frac{1}{\xi_k}}(z) = \frac{\Gamma(k, A_{b1}z^{-\delta})}{\Gamma(k)}, \tag{8.6b}$$

where $A_{b1} = A_{b0}/\delta$.

Proof. See Appendix IV.4. □

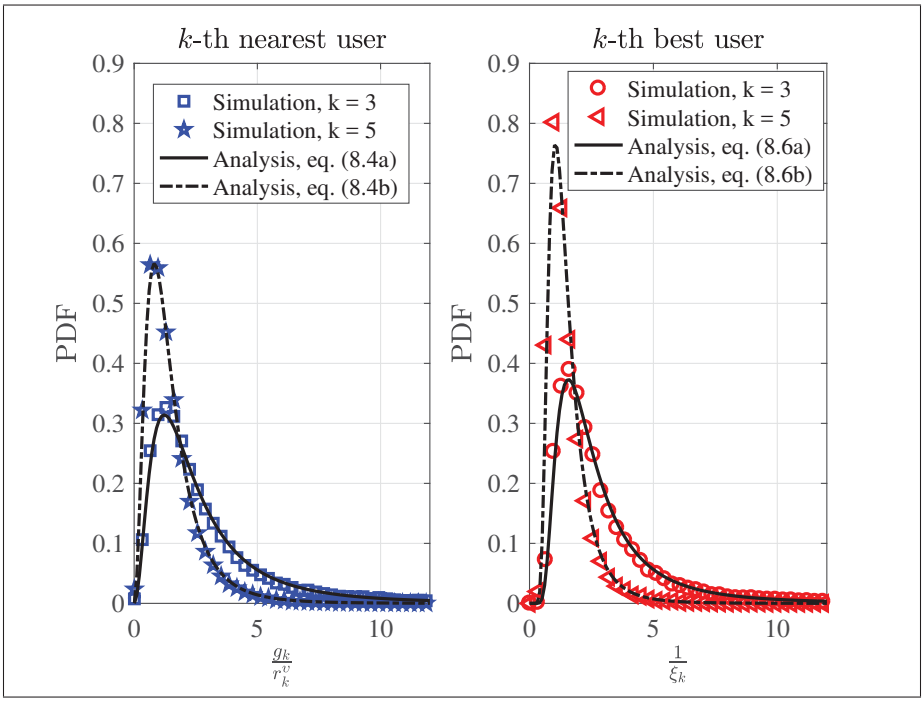


Figure 8.2 The PDFs for the k-th best and nearest users when $\alpha_k = 2$, $\mu_k = 3$, $\eta_k = 0$ dB, $d = \upsilon = 2$, $\lambda_b = 2$, $N_a = N_b = 1$

As shown in Fig. 8.2, the PDFs for the k-th nearest and the k-th best legitimate user are respectively demonstrated, it is observed that our analysis are successfully validated by simulation results.

8.4.2 Secrecy Metrics

8.4.2.1 Connection outage probability

Connection outage probability is defined as the event in which the legitimate receiver cannot successfully decode the transmitted messages. This happens when the main channel capacity falls below the actual transmission rate R_t. It is mathematically defined as

$$\mathscr{P}_{co}(R_t) = \mathscr{P}r\left(\log_2\left(1+\frac{\eta_k g_k}{r_l^{\upsilon}}\right) < R_t\right). \tag{8.7}$$

8.4.2.2 Probability of non-zero secrecy capacity

The secrecy capacity of the aforementioned system model under the assumption that eavesdroppers do not collude, is Liu *et al.* (2014)

$$C_{s:k} = \left[\log_2\left(1+\frac{\eta_k g_k}{r_l^{\upsilon}}\right) - \log_2\left(1+\frac{\eta_e g_e}{r_e^{\upsilon}}\right)\right]^+. \tag{8.8}$$

When the wiretap channel capacity is less than the main channel capacity, the eavesdroppers are incapable of successfully decoding the transmitted messages. The probability of the occurrence for this event is called as the probability of non-zero secrecy capacity. Mathematically from (8.8), the probability of non-zero secrecy capacity is defined as

$$\mathscr{P}_{nz} = \mathscr{P}r\left(\frac{\eta_k g_k}{r_l^{\upsilon}} > \frac{\eta_e g_e}{r_e^{\upsilon}}\right). \tag{8.9}$$

8.4.2.3 Ergodic secrecy capacity

In line with Chen & Yin (2013); Kong *et al.* (2018b); Li, N., Tao, X. & Xu, J. (2014); Li, N., Tao, X., Wu, H., Xu, J. & Cui, Q. (2016); Liu *et al.* (2016); Zhou, X. & McKay, M. R. (2010),

the ergodic secrecy capacity is obtained as follows

$$C_{s:k} = \left[\underbrace{\mathbb{E}\left[\log_2\left(1+\frac{\eta_k g_k}{r_l^{\upsilon}}\right)\right]}_{R_k^M} - \underbrace{\mathbb{E}\left[\log_2\left(1+\frac{\eta_e g_e}{r_e^{\upsilon}}\right)\right]}_{R_k^W} \right]^+, \tag{8.10}$$

where R_k^M and R_k^W are the ergodic capacity of the transmitter to the k-th legitimate receiver and the k-th eavesdropper, respectively.

8.5 Performance Characterization

By using the PDFs and CDFs of the composite channel gain for the k-th nearest/best user, we study the COP, PNZ, and ergodic secrecy capacity, respectively.

8.5.1 Performance Characterization of the COP

8.5.1.1 Connection outage probability for the k-th nearest receiver

From the definition, the COP for the k-th nearest legitimate receiver is mathematically expressed as

$$\mathscr{P}_{co,N}(R_t) = \mathscr{P}r\left(\log_2\left(1+\frac{\eta_k g_k}{r_k^{\upsilon}}\right) < R_t\right) = \mathscr{P}r\left(\frac{g_k}{r_k^{\upsilon}} < \frac{2^{R_t}-1}{\eta_k}\right). \tag{8.11}$$

Notably, $\mathscr{P}_{co,N}(R_t)$ can be assessed from the PDF of the k-th legitimate receiver's channel gain. For the ease of notations, we set $\Delta = \frac{2^{R_t}-1}{\eta_k}$.

Proposition 5. *The COP of the k-th nearest legitimate receiver is given as*

$$\mathscr{P}_{co,N}(R_t) = F_{\frac{g_k}{r_k^{\upsilon}}}(\Delta). \tag{8.12}$$

Proof. Substituting (8.4b) into (8.11), the proof is achieved. □

8.5.1.2 Connection outage probability for the k-th best receiver

Similarly, the COP for the k-th best receiver is given

$$\mathscr{P}_{co,B}(R_t) = \mathscr{P}r\left(\log_2\left(1+\frac{\eta_k}{\xi_k}\right) < R_t\right) = 1 - \mathscr{P}r\left(\xi_k < \frac{1}{\Delta}\right). \tag{8.13}$$

Based on (8.13), it is becoming apparent that the COP for the k-th best receiver is termed as F_{ξ_k}.

Proposition 6. *The COP of the k-th best legitimate receiver takes the following shape*

$$\mathscr{P}_{co,B}(R_t) = \frac{\Gamma\left(k, A_{b1}\Delta^{-\delta}\right)}{\Gamma(k)}. \tag{8.14}$$

Proof. Substituting (8.6b) into (8.13), the proof is completed. □

8.5.2 Performance Characterization of the PNZ

In this section, the PNZs, with respect to the k-th nearest and best legitimate receiver, are well investigated.

As seen from (8.8) for the non-colluding eavesdroppers, the non-zero secrecy capacity for the k-th legitimate receiver is mathematically guaranteed with the probability given for the following four scenarios:

- case 1): the k-th nearest legitimate receiver in the presence of the 1st nearest eavesdropper[5];

$$\mathscr{P}_{nz,NN} = \mathscr{P}r\left(\frac{\eta_k g_k}{r_k^{\upsilon}} > \frac{\eta_e g_e}{r_e^{\upsilon}}\right) = \mathscr{P}r\left(\frac{g_e}{r_e^{\upsilon}}\frac{r_k^{\upsilon}}{g_k} < \frac{\eta_k}{\eta_e}\right) = \int_0^{\infty} F_{\frac{g_e}{r_e^{\upsilon}}}(\varpi y) f_{\frac{g_k}{r_k^{\upsilon}}}(y)\, dy. \tag{8.15}$$

[5] The nearest eavesdropper is the one closest to the legitimate receiver.

- case 2): the k-th best legitimate receiver in the presence of the 1st best eavesdropper[6];

$$\mathscr{P}_{nz,BB} = \mathscr{P}r\left(\frac{\eta_k}{\xi_k} > \frac{\eta_e}{\xi_e}\right) = 1 - \mathscr{P}r\left(\frac{\xi_e}{\xi_k} < \frac{1}{\varpi}\right) = 1 - \int_0^\infty F_{\xi_e}\left(\frac{y}{\varpi}\right) f_{\xi_k}(y)dy. \quad (8.16)$$

- case 3): the k-th nearest legitimate receiver in the presence of the 1st best eavesdropper;

$$\mathscr{P}_{nz,NB} = Pr\left(\frac{\eta_k g_k}{r_k^\upsilon} > \frac{\eta_e}{\xi_e}\right) = 1 - Pr\left(\frac{g_k}{r_k^\upsilon}\xi_e < \frac{1}{\varpi}\right) = 1 - \int_0^\infty F_{\frac{g_k}{r_k^\upsilon}}\left(\frac{1}{\varpi y}\right) f_{\xi_e}(y)dy. \quad (8.17)$$

- case 4): the k-th best legitimate receiver in the presence of the 1st nearest eavesdropper

$$\mathscr{P}_{nz,BN} = Pr\left(\frac{\eta_k}{\xi_k} > \frac{\eta_e g_e}{r_e^\upsilon}\right) = Pr\left(\frac{g_e}{r_e^\upsilon}\xi_k < \varpi\right) = \int_0^\infty F_{\frac{g_e}{r_e^\upsilon}}\left(\frac{\varpi}{y}\right) f_{\xi_k}(y)dy. \quad (8.18)$$

8.5.2.1 The k-th nearest receiver & the 1st nearest eavesdropper

Proposition 7. *The PNZ of the k-th nearest legitimate receiver in the presence of the 1st nearest eavesdropper can be calculated from*

$$\mathscr{P}_{nz,NN} = 1 - \frac{\varepsilon_k \varepsilon_e}{\theta_k \theta_e \Gamma(k)} H_{3,3}^{3,2}\left[\frac{\theta_e \varpi}{\theta_k}\left(\frac{A_k}{A_e}\right)^{\frac{1}{\delta}} \middle| \begin{matrix}(1,1),(1-\mu_k,\frac{2}{\alpha_k}),(0,\frac{1}{\delta}) \\ (0,1),(\mu_e,\frac{2}{\alpha_e}),(k,\frac{1}{\delta})\end{matrix}\right]. \quad (8.19)$$

Proof. See Appendix IV.5. □

8.5.2.2 The k-th best receiver & the 1st best eavesdropper

Proposition 8. *The PNZ of the k-th best legitimate receiver in the presence of the 1st best eavesdropper is given as*

$$\mathscr{P}_{nz,BB} = \left(\frac{A_{b1}}{A_{b1} + A_{e1}\varpi^{-\delta}}\right)^k. \quad (8.20)$$

[6] The best eavesdropper is supposed to be the one with the smallest ξ_e.

Proof. Motivated by (A IV-6), for the best eavesdropper, the CDF of ξ_e is given by

$$\begin{aligned} F_{\xi_e}(x) &= \gamma\left(1, A_{e1}x^{\delta}\right) \\ &= 1-\exp(-A_{e1}x^{\delta}), \end{aligned} \tag{8.21}$$

where $A_{e1} = A_{e0}/\delta$.

After plugging (8.21) and (A IV-7) into (8.16), it yields

$$\begin{aligned} \mathscr{P}_{nz,BB} &= 1-\mathscr{P}r\left(\frac{\xi_e}{\xi_k} < \frac{1}{\varpi}\right) \\ &= 1-\int_0^{\infty} F_{\xi_e}\left(\frac{y}{\varpi}\right) f_{\xi_k}(y)dy \\ &= \int_0^{\infty} \exp\left(-A_{e1}\left(\frac{y}{\varpi}\right)^{\delta}\right)\exp(-A_{b1}y^{\delta})\frac{\delta(A_{b1}y^{\delta})^k}{y\Gamma(k)}dy \\ &\overset{(a)}{=} \frac{\delta A_{b1}^k}{\Gamma(k)}\int_0^{\infty}\exp\left(-(A_{b1}+A_{e1}\varpi^{-\delta})y^{\delta}\right)y^{\delta k-1}dy \\ &= \left(\frac{A_{b1}}{A_{b1}+A_{e1}\varpi^{-\delta}}\right)^k, \end{aligned} \tag{8.22}$$

where (a) follows from (Gradshteyn & Ryzhik, 2014, Eq. (3.351.3)). □

In the following lemma we characterize a limit on the k-th best receiver. From Proposition 8, one can obtain the maximum possible k-th index for a given probability constraint, $\tau = 1-\mathscr{P}_{nz,BB}$.

Lemma 4. *The maximum number of ordered best intended receivers that can securely communicate with the source in the presence of the best eavesdropper is given as*

$$k^* = \log_{\frac{A_{b1}}{A_{b1}+A_{e1}\varpi^{-\delta}}}(\tau). \tag{8.23}$$

Proof. The proof directly follows from Proposition 8. □

8.5.2.3 The k-th nearest receiver & the 1st best eavesdropper

Proposition 9. *The PNZ of the k-th nearest legitimate receiver in the presence of the 1st best non-colluding eavesdropper is given by*

$$\mathscr{P}_{nz,NB} = \frac{\varepsilon_k}{\theta_k \Gamma(k)} H_{3,2}^{1,3}\left[\frac{\varpi}{\theta_k}\left(\frac{A_k}{A_{e1}}\right)^{\frac{1}{\delta}}\middle|\begin{matrix}(1,1),(1-\mu_k,\frac{2}{\alpha_k}),(0,\frac{1}{\delta})\\(k,\frac{1}{\delta}),(0,1)\end{matrix}\right]. \tag{8.24}$$

Proof. See Appendix IV.6. □

8.5.2.4 The k-th best receiver & the 1st nearest eavesdropper

Proposition 10. *The PNZ of the k-th best legitimate receiver in the presence of the 1st nearest non-colluding eavesdropper is given by*

$$\mathscr{P}_{nz,BN} = 1 - \frac{\varepsilon_e}{\theta_e \Gamma(k)} H_{3,2}^{1,3}\left[\frac{1}{\theta_e \varpi}\left(\frac{A_e}{A_{b1}}\right)^{\frac{1}{\delta}}\middle|\begin{matrix}(1,1),(1-\mu_e,\frac{2}{\alpha_e}),(1-k,\frac{1}{\delta})\\(1,\frac{1}{\delta}),(0,1)\end{matrix}\right]. \tag{8.25}$$

Proof. See Appendix IV.7. □

8.5.3 Performance Characterization of Ergodic Secrecy Capacity

From the perspective of the eavesdroppers' received signal quality, the first nearest or best eavesdropper can achieve the highest composite channel gain. As such, the ergodic secrecy capacity can be similarly analyzed for the four considered scenarios. Motivated from (8.10), the ergodic secrecy capacity can be obtained from the difference of the ergodic capacities between the transmitter-legitimate receiver link and the transmitter-eavesdropper link Liu *et al.* (2016). In accordance with our proposed user association method, i.e., the k-th nearest or best user, the ergodic capacity of the transmitter to the k-th nearest legitimate receiver, $R_{N,k}^{M}$, and the transmitter to the k-th best legitimate receiver, $R_{B,k}^{M}$, are correspondingly obtained in the follow proposition in order to simplify our derivations of ergodic secrecy capacity.

Proposition 11. *The ergodic capacity of the transmitter to the k-th nearest or best legitimate user, $R^M_{N,k}$ and $R^M_{B,k}$, are respectively given by*

$$R^M_{N,k} = \frac{\varepsilon_k}{\theta_k \Gamma(k) \ln 2} H^{2,3}_{3,3}\left[\frac{\eta_k A_k^{\frac{1}{\delta}}}{\theta_k} \middle| \begin{matrix} (1,1),(1,1),(1-\mu_k,\frac{2}{\alpha_k}) \\ (1,1),(k,\frac{1}{\delta}),(0,1) \end{matrix} \right], \tag{8.26a}$$

$$R^M_{B,k} = \frac{\delta}{\Gamma(k) \ln 2} H^{2,2}_{3,2}\left[A_{b1} \eta_k^{\delta} \middle| \begin{matrix} (1,\delta),(1,\delta)) \\ (k,1),(1,\delta),(0,\delta) \end{matrix} \right], \tag{8.26b}$$

where $H^{m,n}_{p,q}[.]$ is the Fox's H-function.

Proof. See Appendix. IV.8. □

Similarly, the $R^W_{N,k}$ and $R^W_{B,k}$ can be easily derived by making some simple manipulations. Accordingly, considering either the 1st nearest or best eavesdropper, by letting $k = 1$ for $R^W_{N,k}$ and $R^W_{B,k}$, and setting $R^W_{N,1}$ and $R^W_{B,1}$ as R^W_N and R^W_B, then we have the following remark.

Remark 10. Taking account of the aforementioned four scenarios, the ergodic secrecy capacity are respectively given by

- *case 1:*

$$\bar{C}_{s:k,NN} = [R^M_{N,k} - R^W_N]^+, \tag{8.27a}$$

- *case 2:*

$$\bar{C}_{s:k,BB} = [R^M_{B,k} - R^w_B]^+, \tag{8.27b}$$

- *case 3:*

$$\bar{C}_{s:k,NB} = [R^M_{N,k} - R^W_B]^+, \tag{8.27c}$$

- *case 4:*

$$\bar{C}_{s:k,BN} = [R^M_{B,k} - R^W_N]^+. \tag{8.27d}$$

For the sake of showing brevity, the details are not given in (8.27a-8.27d), respectively, however, those can be easily obtained from Proposition. 11 by making some simple algebraic substitutions.

8.6 Numerical Results and Discussions

For a given network configuration, the secrecy metrics, including the COP and PNZ, are under analysis in Section 8.5. In this section, the accuracy of our analysis is validated by presenting numerical simulations. In the whole simulation configuration, it is assumed that $r = 10$ and the simulation solely takes places under $\alpha - \mu$ fading channels.

In addition, we will study the effects of the density, the path-loss exponent υ, different $\alpha - \mu$ fading factors and dimensions of space on the secrecy metrics. Note that in our simulation, the WAFO toolbox of MATLAB Brodtkorb *et al.* (2000) has been used to generate $\alpha - \mu$ variates.

It is very important to note that higher system performance is achieved at lower COP as well as higher PNZ probabilities.

8.6.1 Results Pertaining to COP

This subsection studies the system performance with respect to the nearest and best legitimate receivers, and we provide a comparison between the two performances.

The $\mathscr{P}_{co,N}$ stated in (8.11) versus the k-th nearest legitimate receiver under $\alpha - \mu$ fading is shown in Fig. 8.3. It demonstrates how the COP for the k-th nearest legitimate receiver is affected as the legitimate user's index increases, for various $\alpha - \mu$ fading scenarios. In addition, Fig. 8.3 also demonstrates the conformity of our analytical derivations to simulation outcomes.

The $\mathscr{P}_{co,B}$ drafted in (8.13) versus λ_b is illustrated and compared with the $\mathscr{P}_{co,B}$ in Fig. 8.4 for selected values of the k-th legitimate nearest/best receiver. From this graph, we obtain the conclusions that: (i) the connection outage occurs with a higher probability for larger index

values and larger λ_b; and (ii) since λ_b grows in equal steps, the gap between $\mathscr{P}_{co,N}$ and $\mathscr{P}_{co,B}$ tends to be larger for higher index values λ_b.

Having studied the performance with respect to the nearest and best legitimate receivers, we compare the COP for the 1st nearest and best legitimate receiver for various selected path-loss exponent υ values and N_b, in the next step.

The result of this comparison is shown in Fig. 8.5. Strikingly, one can conceive that on one hand, higher path-loss exponent always results in a higher probability of connection outage both for the k-th nearest and best receivers. On the other hand, the k-th best receiver always owns a relatively lower connection outage probability compared with the k-th nearest one, as predicted. In addition, the COP deserves with lower probability due to its better quality of received signal, as N_b increase.

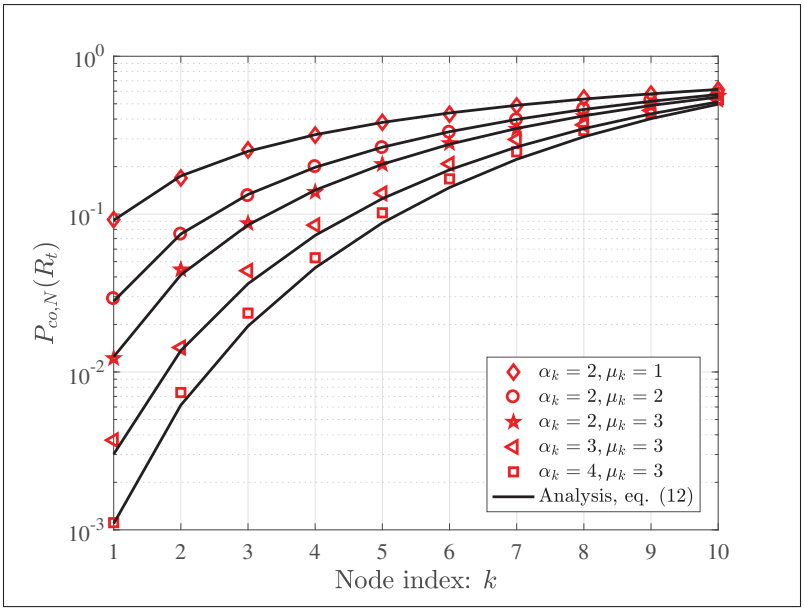


Figure 8.3 $P_{co,N}$ versus the k-th nearest legitimate receiver for $\eta_k = 5$ dB, $\lambda_b = 1$, $N_a = N_b = 1$ $R_t = 1$

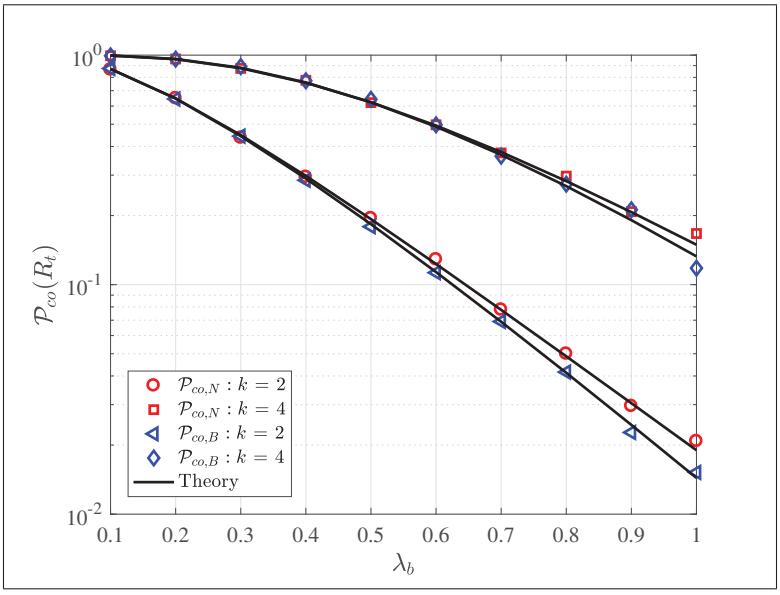


Figure 8.4 P_{co} versus λ_b for selected k-th ($k \in \{2,4\}$) nearest/best user when $\eta_k = 0$ dB, $R_t = 1$, $\alpha_k = 2$, $\mu_k = 3$, $\upsilon = 4$, $d = 2$

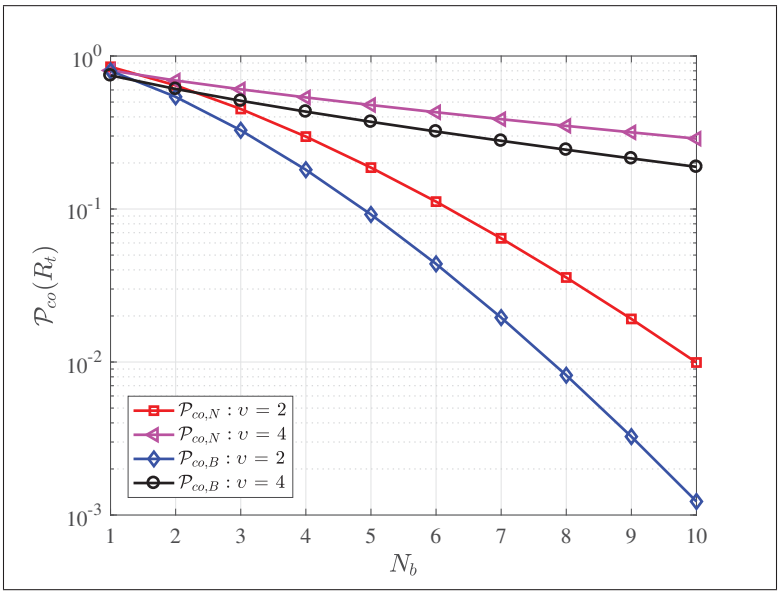


Figure 8.5 Comparison of $\mathscr{P}_{co,N}$ to $\mathscr{P}_{co,B}$ versus N_b for $\lambda_b = 0.1$, $\eta_k = -5$ dB, $\alpha_k = 2$, $\mu_k = 3$, $R_t = 1$, $d = 3$ and various path-loss exponent $\upsilon \in \{2,4\}$

8.6.2 Results Pertaining to PNZ

In this subsection, we study the probability of non-zero secrecy capacity in the presence of non-colluding eavesdroppers. Be reminded that higher PNZ probabilities indicate a better system performance. For the sake of simplicity, the first nearest/best eavesdropper is considered for evaluating the secrecy risk.

Figs. 8.6–8.12 demonstrate the PNZ versus the k-th legitimate receiver in the presence of non-colluding eavesdroppers. It is easily observed that our theoretical analyses are in strong agreement with the simulation outcomes.

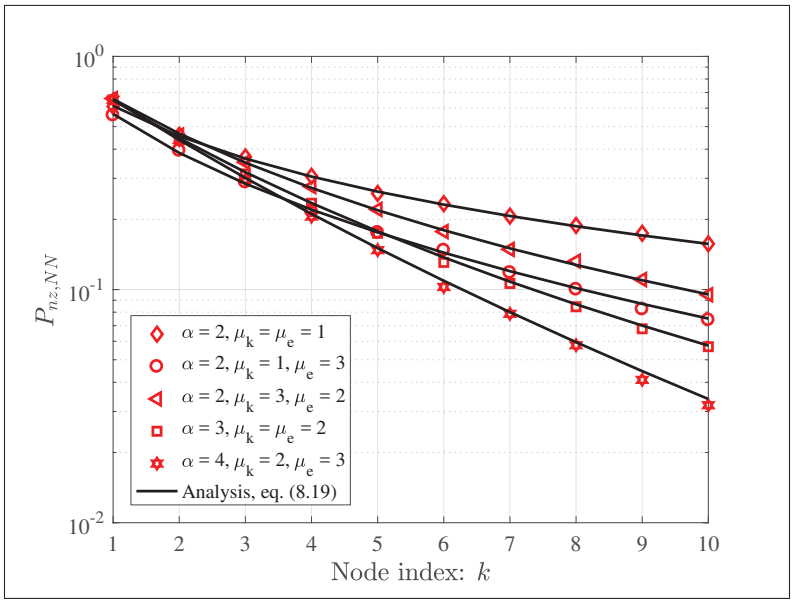


Figure 8.6 $\mathscr{P}_{nz,NN}$ versus the k-th nearest legitimate receiver for $\varpi = 0$ dB, $N_a = N_b = N_e = 1$, $\alpha_k = \alpha_e = \alpha$, $\lambda_b = 0.2$, $\lambda_e = 0.1$, $d = 2$, $\upsilon = 2$

Fig. 8.6 plots the PNZ against the k-th nearest legitimate receiver's index for selected values of α and μ when the nearest eavesdropper is considered. It is observed here that almost for all values of the k-th user index, the PNZ performance is better (probability is higher) for smaller values of α, $\mu_{\rm m}$ and $\mu_{\rm w}$.

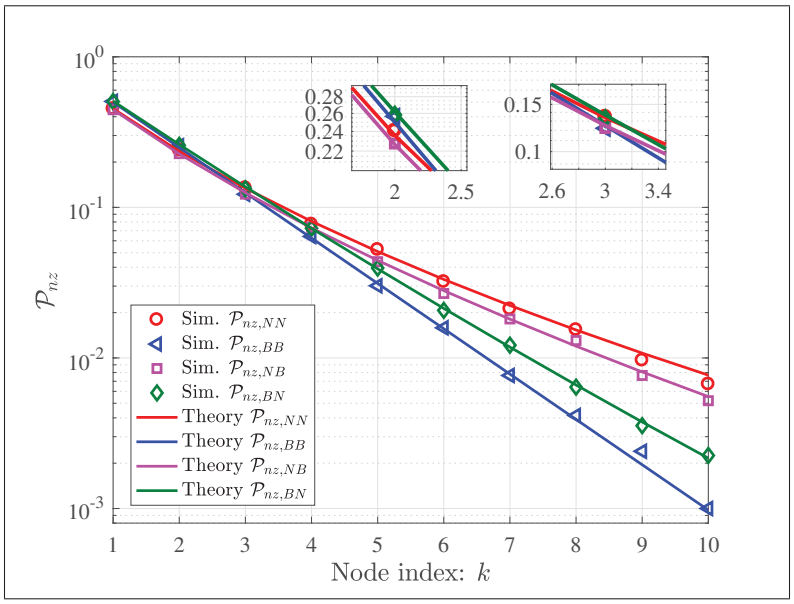


Figure 8.7 $\mathscr{P}_{nz}$ versus the k-th legitimate receiver for $\varpi = 0$ dB, $\lambda_b = 0.2$, $\lambda_e = 0.1$, $N_a = 2, N_b = 1, N_e = 2$, $\alpha_k = 2$, $\mu_k = 1$, $\alpha_e = 2$, $\mu_e = 4$, $d = 2$, $\upsilon = 2$

Fig. 8.7 compares the PNZs given in (8.19), (8.20), (8.24) and (8.25) for the four scenarios, where the 1st nearest or best eavesdropper is considered. One can conceive that (i) our closed-form expressions are confirmed by the Monte-Carlo simulation outcomes; (ii) the $\mathscr{P}_{nz,BN}$ outperforms the other three scenarios when $k = 1, 2$, this trend is changing as k reach 4, the probability of having a positive secrecy capacity drops in a descending order, namely, $\mathscr{P}_{nz,NN} > \mathscr{P}_{nz,NB} > \mathscr{P}_{nz,BN} > \mathscr{P}_{nz,BB}$. The reason behind lies in that two ordering key factors, i.e., distances and composite channel gain, are in turn playing a critical role on the secrecy performance especially as k increases.

As shown in Fig. 8.8, the influence of υ on the PNZ is demonstrated. As it can be readily observed, the PNZs tend to decrease as the k-th user index grows for all considered υ.

Fig. 8.9 presents the maximum number of the k-th best users for a given probability constraint τ. As illustrated in this figure, it can be easily seen that many more best users are permitted for higher ϖ and higher λ_b/λ_e.

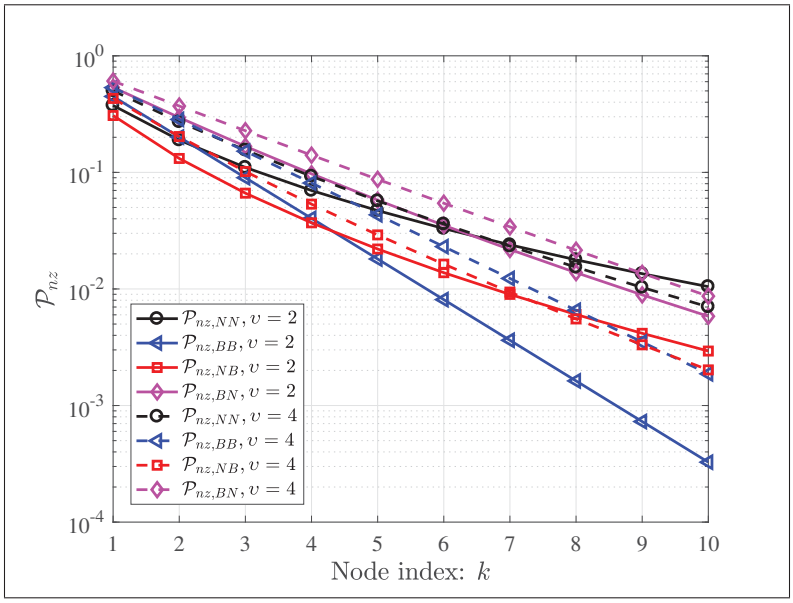


Figure 8.8 $\mathscr{P}_{nz}$ versus the k-th nearest/best legitimate receiver for $\varpi = 0$ dB, $\lambda_b = 0.2$, $\lambda_e = 0.1$, $N_a = 2, N_b = 1, N_e = 2$, $\alpha_k = \alpha_e = \mu_k = 2$, $\mu_e = 3$, and $d = 3$

As observed in Fig. 8.7, the 1st nearest/best legitimate receiver is mostly endangered by the malicious eavesdropper. As a result, in the following three Figs, the impacts of ϖ, the receiving antenna numbers N_b, N_e, and the density of two kinds of receivers, λ_b and λ_e on the PNZ are investigated. In this case, the first nearest/best legitimate receiver is considered in Figs. 8.10-8.12.

In Fig. 8.10, the PNZs are anticipated to witness an increasing trend as ϖ increases. It is intuitively observed that the 1st best user is guaranteed with a higher probability in the presence of the 1st nearest eavesdropper. Such a phenomenon repeats itself for the Figs 8.11 and 8.12.

To terminate the discussion, in Figs. 8.11 and 8.12, we present the PNZs against the number of receiving antennas and the densities, respectively. It is observed that an increased N_b/N_e ratio indicates the legitimate receivers are much more capable to achieve a higher quality of receiving signals, which naturally yields a higher probability of positive secrecy capacity. It is validated by Fig. 8.11(a).

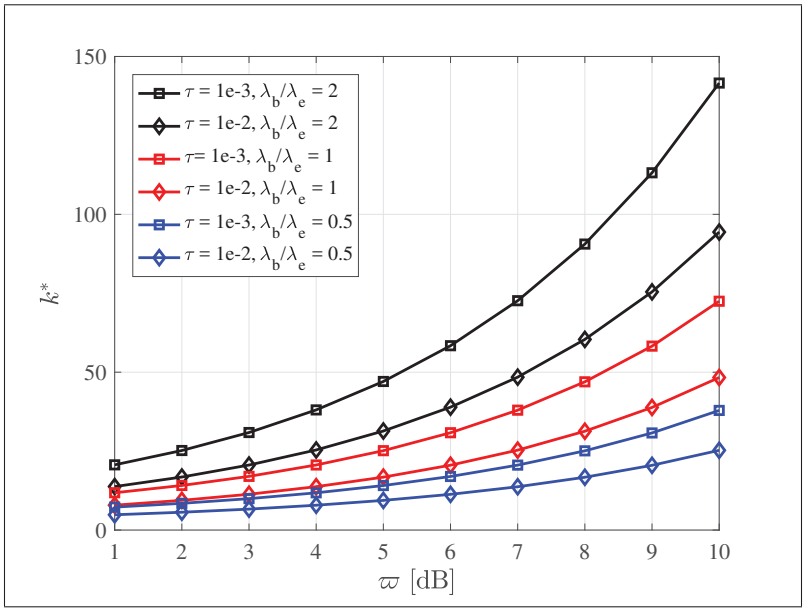


Figure 8.9 The maximum size of the best ordered user k^* versus ϖ for selected values of τ and density ratios λ_b/λ_e, according to (8.23), when $N_a = N_b = N_e = 1$, $\alpha_k = 3, \mu_k = 2$, $\alpha_k = 2, \mu_k = 3$, and $d = \upsilon = 2$

On the contrary, this trend is conversely preserved regardless of the k-th user index value. As N_e/N_b increases, the k-th best legitimate receiver achieves the highest and second-highest probability of non-zero secrecy capacity (best performance), in the presence of the nearest/best eavesdropper, respectively, which are characterized by $\mathscr{P}_{nz,BN}$ and $\mathscr{P}_{nz,BB}$. Next, the 1st nearest legitimate receiver suffers more, resulting in a lower probability, as denoted by $\mathscr{P}_{nz,NN}$. Naturally, the worst performance is recoded when the system challenges against the best eavesdropper, described by $\mathscr{P}_{nz,NB}$.

From the comparison of the PNZ against densities shown in Fig. 8.12, one can conclude that (i) conditioned on a given λ_b, the higher λ_e indicates a system with relatively more eavesdroppers. An increase in the number of eavesdroppers progressively endangers the legitimate link, i.e., probability becomes worse (lower) for higher number of eavesdroppers; and (ii) for a fixed number of eavesdroppers, lower λ_b values result in worse performance, i.e., lower probability of non-zero secrecy capacity.

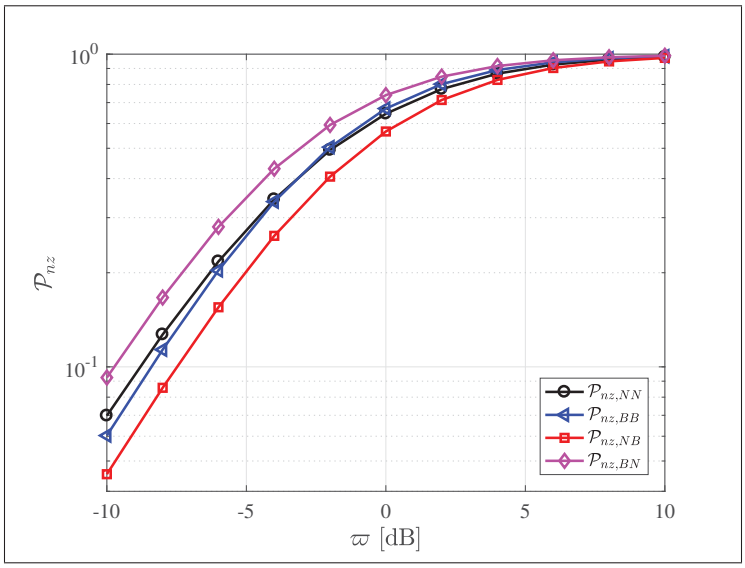


Figure 8.10 $\mathscr{P}_{nz}$ versus ϖ for the 1*st* nearest/best legitimate receiver for $\lambda_b = 0.2$, $\lambda_e = 0.1$, $N_a = N_b = N_e = 2$, $\alpha_k = \alpha_e = 2$, $\mu_k = 2$, $\mu_e = 3$, $d = 3$ and $\upsilon = 2$

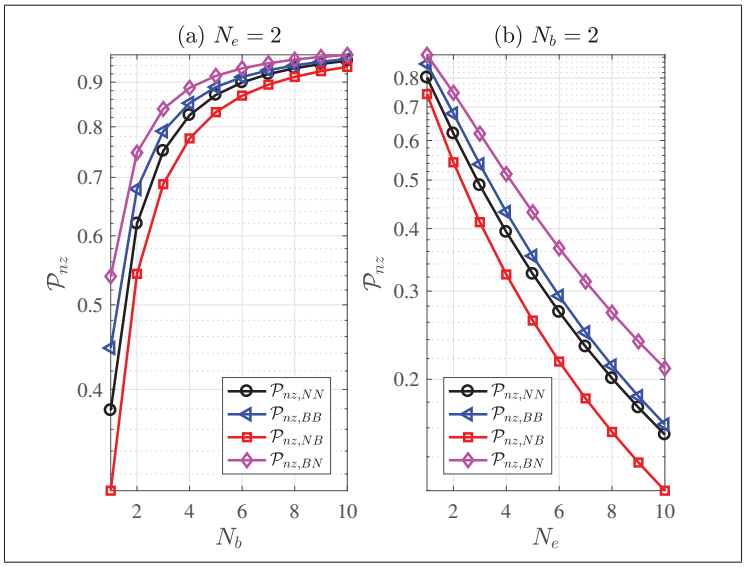


Figure 8.11 $\mathscr{P}_{nz}$ versus the number of received antennas at the 1st nearest/best receivers for $\varpi = 10$ dB, $\lambda_b = 0.2$, $\lambda_e = 0.1$, $\alpha_k = \alpha_e = 2$, $\mu_k = 1$, $\mu_e = 3$, $d = 3$, $N_a = 2$ and $\upsilon = 2$

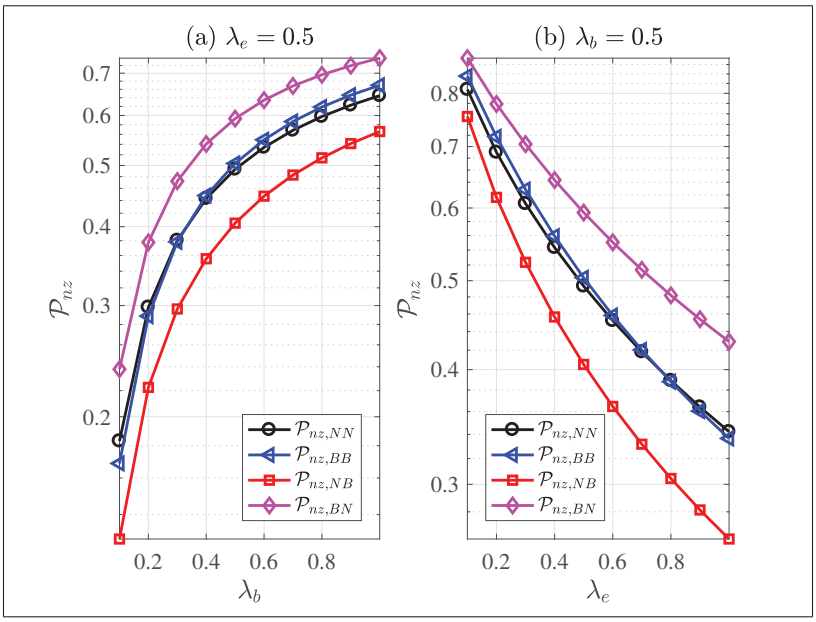


Figure 8.12 $\mathscr{P}_{nz}$ versus the density of 1st nearest/best receivers for $\varpi = 10$ dB, $N_a = N_b = N_e = 2$, $\alpha_k = \alpha_e = 2$, $\mu_k = 2$, $\mu_e = 3$, $d = 3$ and $\upsilon = 2$

8.6.3 Results Pertaining to Ergodic Secrecy Capacity

Fig. 8.13 plots the ergodic secrecy capacity versus the k-th nearest or best legitimate receiver, while in the presence of the 1st nearest or best eavesdropper, respectively. Again, the same conclusion can be obtained: the ergodic secrecy capacity, as depicted in case 4, outperforms the other 3 cases.

8.7 Conclusion

In the context of this paper, we investigated the secrecy performance of HPPP-based random MIMO wireless networks over $\alpha - \mu$ fading channels for the first time. For the purpose of evaluating the secrecy performance of such a network, the COP, PNZ and ergodic secrecy capacity for the k-th nearest/best legitimate receiver in the presence of non-colluding eavesdroppers are derived and quantified with closed-form expressions.

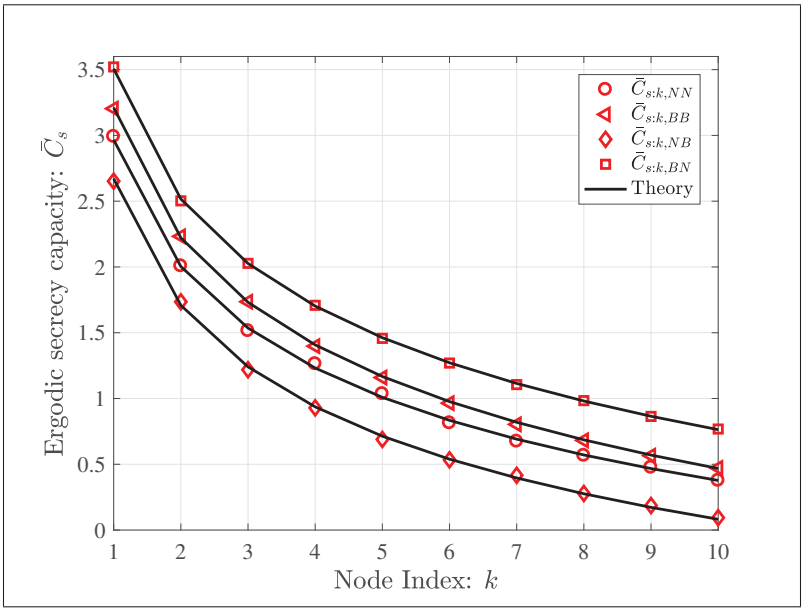


Figure 8.13 $\bar{C}_s$ versus the k-th nearest/best legitimate receiver for $\lambda_b = \lambda_e = 1$, $N_a = N_b = N_e = 1$, $\alpha_k = \alpha_e = 2$, $\mu_k = \mu_e = 1$, $d = 2$ and $\upsilon = 2$, $\eta_k = 15$ dB, $\eta_e = 0$ dB

The accuracy of our analytical derivations are further successfully confirmed by simulation outcomes. Remarkable observations are drawn from the numerical results obtained in this paper. Indeed, the secrecy performance metrics are influenced by the density of users, the path-loss exponent, the number of transmitting and receiving antennas, as well as the fading parameters. In addition, the secrecy performance regarding the k-th best legitimate receiver outperforms that of the k-th nearest one. Hence, the nearest path does not necessarily provide the best secrecy performance. This paper's results and outcomes regarding parameters that influence secrecy performance will enable researchers or wireless system designers to quickly evaluate system performance and determine the optimal available parameter choices when facing different security risks. Finally, inspired from Wang, G., Liu, Q., He, R., Gao, F. & Tellambura, C. (2015b), future works will focus on using the beamforming deploying artificial noise technique over the homogeneous stochastic MIMO wireless network.

CONCLUSION AND RECOMMENDATIONS

9.1 Conclusions

The aim of this dissertation is the secrecy characterization of physical layer security over the $\alpha-\mu$, Fisher-Snedecor $\mathscr{F}$, and Fox's H-function wiretap fading channels. Conclusively speaking, there are four main contributions in this dissertation: (i) secrecy investigation over three fading models, where secrecy metrics are derived with closed-form expressions; (ii) exploration of physical layer security over wireless fading channels, with the assistance of MG distributions; (iii) reliability and secrecy exploration of a new fading model, i.e., the cascaded $\alpha-\mu$, and (iv) secrecy evaluation of random MIMO wireless networks over $\alpha-\mu$ fading channels. Specifically, the aforementioned contributions are further detailed as follows:

- The first aspect of this dissertation contains three sub-contributions. Those contributions are organized in accordance with the three fading models, namely, $\alpha-\mu$, Fisher-Snedecor $\mathscr{F}$, and Fox's H-function. The secrecy performance over SISO and SIMO $\alpha-\mu$ wiretap fading channels are provided in Chapters 2 and 3, respectively. Secrecy metrics, including secrecy outage probability and the probability of non-zero secrecy capacity, are both characterized by closed-form expressions. Similarly, secrecy evaluation over Fisher-Snedecor $\mathscr{F}$ and Fox's H-function wiretap fading channels are subsequently conducted in Chapters 4 and 5, respectively. The exact and asymptotic behaviors of secrecy metrics are also provided. In addition, the MG distribution was deployed in Chapter 6 to analyze the secrecy metrics.

- In continuation with the secrecy characterization over $\alpha-\mu$ wiretap fading channels, in Chapter 7, the cascaded $\alpha-\mu$ fading channel was proposed. This new fading model can be used to characterize several wireless communication scenarios, such as multi-hop AF relaying networks and MIMO keyhole communication systems. The key contributions of Chapter 7 are two-fold: (i) mathematical characteristics of the cascaded $\alpha-\mu$ distribution;

and (ii) feasibility and applicability of this model to a wireless communication system, in other words, reliability and secrecy analysis over cascaded $\alpha - \mu$ fading channels.

- The aforementioned chapters considered the secrecy analysis over three fading channels. On account of the realistic wireless communication system, i.e., the impacts from the spatial distribution of users, the path-loss exponent, the number of antennas, and the density of users, secrecy exploration of random MIMO wireless networks over $\alpha - \mu$ wiretap fading channels was studied in Chapter 8. The legitimate and malicious users are respectively modeled with two independent HPPPs. The connection outage probability, the probability of non-zero secrecy capacity, and the ergodic secrecy capacity were derived with closed-form expressions. This work enables wireless communication engineers to have quick access and thus to perform secrecy evaluations when facing security risks.

9.2 Future work

In this dissertation, the contributions presented could be extended to the following future directions:

9.2.1 Imperfect CSI, Outdated CSI, and Aging CSI

In this dissertation, assuming the availability of perfect CSI at the transmitters and receivers, secrecy performance was explored over several fading channel models. Actually, the imperfect CSI caused by the channel estimation process, and the outdated and aging CSI caused by the users' mobility, are of high significance to the secrecy performance evaluation. As stated in one of the conference papers entitled 'Secrecy Analysis of A MIMO Full-Duplex Active Eavesdropper with Channel Estimation Errors', it has shown that imperfect CSI degrades the secrecy performance. Also, the works in Hu, J., Yang, W., Yang, N., Zhou, X. & Cai, Y. (2016); Michalopoulos, D. S., Suraweera, H. A., Karagiannidis, G. K. & Schober, R. (2012); Zhao, R.,

Lin, H., He, Y. C., Chen, D. H., Huang, Y. & Yang, L. (2018) investigated the impacts caused by outdated CSI and channel aging on secrecy metrics. As a result, the secrecy performance with consideration of the practical CSI situation is worthwhile to be examined and analyzed in the future.

9.2.2 Unavailability of Eavesdroppers' CSI

Throughout this thesis, it is assumed that the eavesdroppers' CSI is perfectly known at the transmitter. Such an assumption is usually impractical, especially in the presence of passive eavesdroppers. Towards this end, how to elaborate the influences of the uncertainty of the eavesdroppers' CSI into the secrecy exploration will be a promising direction.

9.2.3 Full-duplex Transceivers and Interference

In the aforementioned conference paper, a full-duplex eavesdropper is considered to wiretap the legitimate link while sending jamming signals to the legitimate receiver. From the perspective of legitimate users, jamming signals from illegitimate users are surely regarded as interference to prevent secure transmission of intended private messages. To this end, how to reasonably employ full-duplex techniques and jamming policies at the legitimate users is a promising and interesting research problem to enhance secrecy in wireless networks.

9.2.4 Relaying Scheme and Randomly Distributed Users

In Chapter 8, the legitimate users and eavesdroppers are modeled as two independent HPPPs. Random eavesdroppers are ordered according to the quality of eavesdroppers' received signal or to the distance from the transmitter, to explore how much risk are burdened on the legitimate receivers. Motivated by the results obtained in Chapter 8, a new future research work could be the investigation of multi-hop relaying networks in the presence of random eavesdroppers.

Relaying schemes can be AF or decode-and-forward (DF). Linear and non-linear multi-hop relaying networks can be configured to evaluate the security concern.

APPENDIX I

PROOFS FOR CHAPTER 4

1. Proof for $\mathscr{P}_{out,1}$

In order to obtain the analytical solution to (4.7), the Parseval's relation for Mellin transform (Debnath & Bhatta, 2014, eq. (8.3.23)) is recalled, which is given by

$$\mathscr{P}_{out}(R_t) = \int_0^{\infty} F_B(\gamma_0) f_E(\gamma_E) d\gamma_E = \frac{1}{2\pi j} \int_{\mathscr{L}_1} \mathscr{M}[F_B(\gamma_0), 1-s] \mathscr{M}[f_E(\gamma), s] ds, \tag{A I-1}$$

where $\mathscr{L}_1$ is the integration path from $\upsilon - j\infty$ to $\upsilon + j\infty$, and υ is a constant Debnath & Bhatta (2014).

Then by introducing the definition of univariate Meijer's G-function, $\mathscr{M}[F_B(\gamma_0), 1-s]$ can be rewritten as

$$\begin{aligned} \mathscr{M}[F_B(\gamma_0), 1-s] &= \int_0^{\infty} \gamma_E^{-s} F_B(\gamma_0) d\gamma_E \\ &\overset{(b)}{=} \frac{\Phi_B}{2\pi j} \int_{\mathscr{L}_2} \frac{\Gamma(-\xi)\Gamma(m_B+\xi)\Gamma(m_{B,s}-\xi)}{\Gamma(1-\xi)} \lambda_B^{-\xi} \times \int_0^{\infty} \gamma_E^{-s} \gamma_0^{-\xi} d\gamma_E d\xi, \end{aligned} \tag{A I-2}$$

where step (b) is developed by interchanging the order of two integrals.

The inner integral in (A I-2) can be further written as

$$\begin{aligned} &\int_0^{\infty} \gamma_E^{-s} \gamma_0^{-\xi} d\gamma_E \overset{(c)}{=} \mathscr{W}^{-\xi} \int_0^{\infty} \frac{\gamma_E^{-s}}{\left(1+\frac{R_s}{\mathscr{W}}\gamma_E\right)^{\xi}} d\gamma_E \\ &\overset{(d)}{=} \mathscr{W}^{-\xi} \mathscr{B}(1-s, \xi+s-1) \left(\frac{R_s}{\mathscr{W}}\right)^{s-1} \overset{(e)}{=} \mathscr{W}^{-\xi} \frac{\Gamma(1-s)\Gamma(\xi+s-1)}{\Gamma(\xi)} \left(\frac{R_s}{\mathscr{W}}\right)^{s-1}, \end{aligned} \tag{A I-3}$$

where step (c) is developed by representing $\gamma_0 = R_s\gamma_E + \mathscr{W}$, step (d) is obtained from (Gradshteyn & Ryzhik, 2014, eq. (3.194.3)), and step (e) is further simplified in a closed-form by deploying the property $\mathscr{B}(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$ (Gradshteyn & Ryzhik, 2014, eq. (8.384.1)).

Next, plugging (A I-3) into (A I-2), yields the following result

$$\begin{aligned}\mathscr{M}[F_B(\gamma_0),1-s] &= \frac{\Phi_B}{2\pi j}\int_{\mathscr{L}_2}\frac{\Gamma(-\xi)\Gamma(m_B+\xi)}{\Gamma(1-\xi)}\frac{\Gamma(m_{B,s}-\xi)\Gamma(1-s)\Gamma(\xi+s-1)}{\Gamma(\xi)(\lambda_B\mathscr{W})^{\xi}}\left(\frac{R_s}{\mathscr{W}}\right)^{s-1}d\xi \\ &= \frac{\Phi_B\Gamma(1-s)R_s^{s-1}}{\mathscr{W}^{s-1}}G_{3,3}^{2,2}\left[\lambda_B\mathscr{W}\left|\begin{matrix}(1-m_{B,s},1,0)\\(s-1,m_B,0)\end{matrix}\right.\right],\end{aligned} \tag{A I-4}$$

where $\mathscr{L}_2$ is a certain contour, which separates the poles of $\Gamma(-\xi)$ from the poles of $\Gamma(m_B+\xi)$.

In continuation, with the help from (Mathai *et al.*, 2009a, eq. (2.9)), $\mathscr{M}[f_E(\gamma),s]$ is given by

$$\mathscr{M}[f_E(\gamma_E),s] = \mathscr{C}_E\frac{\Gamma(m_E-1+s)\Gamma(1+m_{E,s}-s)}{\lambda_E^s}. \tag{A I-5}$$

Next, substituting (A I-4) and (A I-5) into (A I-1), yields

$$\begin{aligned}\mathscr{P}_{out} = -\frac{\Phi_B\mathscr{C}_E\mathscr{W}}{4\pi^2R_s}\int_{\mathscr{L}_1}\int_{\mathscr{L}_2}&\frac{\Gamma(\xi+s-1)\Gamma(-\xi)}{\Gamma(1-\xi)\Gamma(\xi)}\Gamma(m_{B,s}-\xi)\Gamma(m_B+\xi)\Gamma(1-s)\\ &\times\Gamma(m_E-1+s)\Gamma(1+m_{E,s}-s)\left(\frac{R_s}{\lambda_E\mathscr{W}}\right)^{s}\left(\frac{1}{\lambda_B\mathscr{W}}\right)^{\xi}d\xi ds,\end{aligned} \tag{A I-6}$$

subsequently, applying the definition of bivariate Meijer's *G*-function results in the accomplishment of the proof.

2. Proof for $\mathscr{P}_{out,2}$

By substituting (4.5) and (4.3) into (4.7), making change of variables $\lambda_B R_s\gamma_E = y$, then we have

$$\mathscr{P}_{out} = \frac{\Phi_B\mathscr{C}_E}{\lambda_B R_s}\int_0^{\infty}G_{1,1}^{1,1}\left[\frac{\lambda_E}{\lambda_B R_s}y\left|\begin{matrix}-m_{E,s}\\m_E-1\end{matrix}\right.\right]G_{2,2}^{1,2}\left[y+\lambda_B\mathscr{W}\left|\begin{matrix}(1-m_{B,s},1)\\(m_B,0)\end{matrix}\right.\right]dy, \tag{A I-7}$$

next, using (Prudnikov *et al.*, 1990, eq.(2.24.1.3)), we complete the proof.

APPENDIX II

PROOFS FOR CHAPTER 5

1. Proof of the Theorem 4

At the very beginning, revisiting (5.12a)

$$\begin{aligned}\mathscr{P}_{out} &= \int_0^{\infty} F_B(\gamma_0) f_E(\gamma_E) d\gamma_E \\ &= 1 - \int_0^{\infty} \bar{F}_B(\gamma_0) f_E(\gamma_E) d\gamma_E \\ &= 1 - \frac{1}{2\pi j} \int_{\mathscr{L}_1} \mathscr{M}[\bar{F}_B(\gamma_0), 1-s] \mathscr{M}[f_E(\gamma_E), s] ds,\end{aligned} \tag{A II-1}$$

and using the definition of Mellin transform and Fox's H-function, we arrive at $\mathscr{M}[F_B(s)]$

$$\begin{aligned}\mathscr{M}[F_B(\gamma_0), 1-s] &= \int_0^{\infty} \gamma_E^{-s} F_B(\gamma_0) d\gamma_E \\ &\overset{(a)}{=} \frac{\kappa_B}{2\lambda_B \pi j} \int_{\mathscr{L}_1} \Theta_B^F(\xi) \lambda_B^{-\xi} \int_0^{\infty} \gamma_E^{-s} \gamma_0^{-\xi} d\gamma_E d\xi,\end{aligned} \tag{A II-2}$$

where step (a) is developed by interchanging the order of two integrals. The inner integral in (A II-2) can be further expressed as

$$\begin{aligned}\int_0^{\infty} \gamma_E^{-s} \gamma_0^{-\xi} d\gamma_E &= \mathscr{W}^{-\xi} \int_0^{\infty} \gamma_E^{-s} \left(1 + \frac{R_s}{\mathscr{W}} \gamma_E\right)^{-\xi} d\gamma_E \\ &\overset{(b)}{=} \frac{\mathscr{B}(1-s, \xi+s-1)}{\mathscr{W}^{\xi}} \left(\frac{R_s}{\mathscr{W}}\right)^{s-1} \\ &\overset{(c)}{=} \frac{\Gamma(1-s)\Gamma(\xi+s-1)}{\Gamma(\xi)\mathscr{W}^{\xi} \left(\frac{R_s}{\mathscr{W}}\right)^{1-s}},\end{aligned} \tag{A II-3}$$

where step (b) is developed from (Gradshteyn & Ryzhik, 2014, eq. (3.194.3)), and step (c) is obtained by using $\mathscr{B}(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$ (Gradshteyn & Ryzhik, 2014, eq. (8.384.1)).

Plugging (A II-3) into (A II-2), yields the result given in (A II-4),

$$\begin{aligned}\mathscr{M}[F_B(\gamma_0),1-s] &\overset{(d)}{=} \frac{\kappa_B}{2\lambda_B\pi j}\left(\frac{R_s}{\mathscr{W}}\right)^{s-1}\Gamma(1-s)\int_{\mathscr{L}_1}\frac{\Gamma(\xi+s-1)\Theta_B^F(\xi)}{\Gamma(\xi)}(\lambda_B\mathscr{W})^{-\xi}d\xi \\ &= \frac{\kappa_B\Gamma(1-s)}{\lambda_B}\left(\frac{R_s}{\mathscr{W}}\right)^{s-1} H_{p_1+2,q_1+2}^{m_1+1,n_1+1}\left[\lambda_B\mathscr{W}\left|\begin{matrix}(1,1),(a_j+A_j,A_j)_{j=1:p},(0,1)\\(s-1,1),(b_j+B_j,B_j)_{j=1:q},(0,1)\end{matrix}\right.\right],\end{aligned} \tag{A II-4}$$

and step (d) is directly achieved from the definition of bivariate Fox's H-function.

Subsequently, substituting (A II-4) and $\mathscr{M}[f_E(\gamma_E),s]=\frac{\kappa_E\chi_E^f(s)}{\lambda_E^s}$ into (A II-1), yields the following result

$$\mathscr{P}_{out} = 1-\frac{\kappa_B\kappa_E\mathscr{W}}{4\lambda_B R_s\pi^2}\int_{\mathscr{L}_1}\int_{\mathscr{L}_2}\frac{\Gamma(\xi+s-1)\Theta_B^{\bar{F}}(\xi)}{\Gamma(\xi)\,(\lambda_B\mathscr{W})^{\xi}}\Gamma(1-s)\Theta_E^f(s)\left(\frac{R_s}{\lambda_E\mathscr{W}}\right)^s d\xi ds, \tag{A II-5}$$

Next, deploying the definition of the bivariate Fox's H-function Gradshteyn & Ryzhik (2014), the proof is achieved.

2. Proof for Theorem 20

Since the logarithm function can be alternatively re-expressed in terms of Fox's H-function with the help from (Prudnikov *et al.*, 1990, eq. (8.4.6.5)) and (Prudnikov *et al.*, 1990, eq. (8.3.2.21)),

$$\ln(1+x) = H_{2,2}^{1,2}\left[x\left|\begin{matrix}(1,1),(1,1)\\(1,1),(0,1)\end{matrix}\right.\right], \tag{A II-6}$$

For the ease of proof, we take the proof for I_1 as an example.

$$I_1 = \frac{1}{2\pi j}\int_{\mathscr{L}_1}\mathscr{M}[F_E(\gamma_B),s]\mathscr{M}[g(\gamma_B),1-s]ds, \tag{A II-7}$$

$$\mathscr{M}[F_E(\gamma_B),s] = \frac{\kappa_E}{\lambda_E^{1+s}}\Theta_E^F(s), \tag{A II-8}$$

where $\Theta_E^F(s)$ is given by

$$\Theta_E^F(s) = \frac{\Gamma(-s)\prod_{l=1}^{m_2}\Gamma(d_l+D_l+D_l s)}{\Gamma(1-s)\prod_{l=m_2+1}^{q_2}\Gamma(1-d_l-D_l-D_l s)}\frac{\prod_{i=1}^{n_2}\Gamma(1-c_i-C_i-C_i s)}{\prod_{i=n_2+1}^{p_2}\Gamma(c_i+C_i+C_i s)}, \tag{A II-9}$$

$\mathscr{M}[g_k(\gamma_k),1-s]$ can be regarded as the Mellin transform of the product of two Fox's H-function (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), which is given by (A II-10)

$$\begin{aligned}\mathscr{M}[g_B(\gamma_B),1-s] &= \int_0^\infty \gamma_B^{-s}\ln(1+\gamma_B)f_B(\gamma_B)d\gamma_B \\ &= \kappa_B\int_0^\infty \gamma_B^{-s}H_{2,2}^{1,2}\left[x\left|\begin{matrix}(1,1),(1,1)\\(1,1),(0,1)\end{matrix}\right.\right]H_{p_1,q_1}^{m_1,n_1}\left[\lambda_B\gamma_B\left|\begin{matrix}(a_j,A_j)_{j=1:p_1}\\(b_j,B_j)_{j=1:q_1}\end{matrix}\right.\right]d\gamma_B \\ &= \frac{\kappa_B}{\lambda_B^{1-s}}H_{q_1+2,p_1+2}^{n_1+1,m_1+2}\left[\frac{1}{\lambda_B}\left|\begin{matrix}(1,1),(1,1),(1-b_j-(1-s)B_j,B_j)_{j=1:q_1}\\(1,1),(1-a_j-(1-s)A_j,A_j)_{j=1:p_1},(0,1)\end{matrix}\right.\right].\end{aligned} \tag{A II-10}$$

Next, substituting (A II-8) and (A II-10) into (A II-7), yields the following result

$$I_1 = -\frac{\kappa_B\kappa_E}{4\pi^2\lambda_B\lambda_E}\int_{\mathscr{L}_1}\int_{\mathscr{L}_2}\frac{\Theta(s,\xi)\Theta(\xi)\Theta_E^F(s)}{\left(\frac{\lambda_E}{\lambda_B}\right)^s\lambda_B^\xi}dsd\xi, \tag{A II-11}$$

where $\Theta(s,\xi)$ and $\Theta(\xi)$ are respectively given by (A II-12a) and (A II-12b)

$$\Theta(s,\xi) = \frac{\prod_{i=1}^{n_1}\Gamma(1-a_i-A_i+A_i s+A_i\xi)\prod_{l=1}^{m_1}\Gamma(b_l+B_l-B_l s-B_l\xi)}{\prod_{i=n_1+1}^{p_1}\Gamma(a_i+A_i-A_i s-A_i\xi)\prod_{l=m_1+1}^{q_1}\Gamma(1-b_l-B_l+B_l s+B_l\xi)}, \tag{A II-12a}$$

$$\Theta(\xi) = \frac{\Gamma(1+\xi)\Gamma(-\xi)\Gamma(-\xi)}{\Gamma(1-\xi)}. \tag{A II-12b}$$

Next, replacing $\xi = -\eta$, $s = -\tau$, I_1 can be expressed as (5.21a) in terms of the bivariate Fox's H-function. In particular, when $n_1 = 0$, I_1 is further simplified in terms of the extended generalized bivariate Fox's H-function.

Following the same methodology, I_2 can be obtained. I_3 can be finally achieved from (Alhennawi *et al.*, 2016, eq. (18)),

$$\begin{aligned} I_3 &= \frac{\kappa_E}{2\pi j}\int_{\mathscr{L}_1} \mathscr{M}\{\ln(1+\gamma_E), s\}\lambda_E^{-1+s}\Theta_E^f(1-s)ds \\ &= \frac{\kappa_E}{\lambda_E} H_{q_2+2,p_2+2}^{n_2+1,m_2+2}\left[\frac{1}{\lambda_E}\middle|\begin{matrix}(1,1),(1,1),(1-d_l-D_l,D_l)_{l=1:p_2}\\ (1,1),(1-c_i-C_i,C_i)_{i=1:q_2},(0,1)\end{matrix}\right]. \end{aligned} \tag{A II-13}$$

3. Proof for Asymptotic ASC

Specifically, at high $\bar{\gamma}_B$ regime, I_1 can be expanded at the pole, i.e., $\xi = 0$, since $\xi = 0$ is the second order pole, as such, by using the residue theorem, we have

$$\text{Res}\left[\frac{\Theta(\text{s},\xi)\Theta(\xi)}{\lambda_{\text{B}}^{\xi}}, 0\right] = \lim_{\xi\to 0}\frac{d}{d\xi}\frac{\xi^2\Theta(s,\xi)\Gamma(\xi)^2\Gamma(1-\xi)}{\lambda_B^{\xi}\Gamma(1+\xi)}. \tag{A II-14}$$

Using the fact that $\frac{d\Gamma(s)}{ds} = \Gamma(s)\Psi_0(s)$ and the general Leibniz rule, we have

$$\begin{aligned} \text{Res}\left[\frac{\Theta(\text{s},\xi)\Theta(\xi)}{\lambda_{\text{B}}^{\xi}}, 0\right] =& \Theta(s,0)\left[\sum_{l=1}^{m_1} B_l\Psi_0(b_l+B_l+B_l s) - \sum_{j=1}^{n_1} A_j\Psi_0(1-a_j-A_j-A_j s)\right. \\ &\left. + \sum_{l=m_l+1}^{q_1} B_l\Psi_0(1-b_l-B_l-B_l s) - \sum_{i=n_1+1}^{p_1} A_i\Psi_0(a_i+A_i+A_i s) - \ln\lambda_B\right], \end{aligned} \tag{A II-15}$$

and subsequently when $\dfrac{\lambda_E}{\lambda_B} \to \infty$, we evaluate the residue at s, where

$$s = \max\left[0, \left(-\frac{b_l+B_l}{B_l}\right)_{l=1,\cdots,m_l}, \left(\frac{c_i+C_i-1}{c_i}\right)_{i=1,\cdots,n_2}\right]. \tag{A II-16}$$

Considering all poles are simple, we arrive at the derived asymptotic I_1.

Similarly, at high $\bar{\gamma}_B$ regime, I_2 can be obtained at the point $u = \min\left(\frac{b_l+B_l}{B_l}\right)_{l=1,\cdots,m_1}$, we complete the proof.

APPENDIX III

PROOFS FOR CHAPTER 7

1. Proof for Asymptotic $\mathscr{P}_{op}$

Rewrite (7.16) in terms of the Fox's H-function, we have

$$\mathscr{P}_{op} = 1 - \frac{\mathscr{K}_N}{2\pi\mathscr{C}j}\int_{\mathscr{L}} \underbrace{\frac{\Gamma(s)\prod_{k=1}^{N}\Gamma\left(\mu_i + \frac{2}{\alpha_k}s\right)}{\Gamma(1+s)\left(\mathscr{K}_N\gamma_{th}\right)^s}}_{\varepsilon(s)} ds. \tag{A III-1}$$

According to Chergui *et al.* (2016), expansions of the univariate and bivariate Fox's H-functions can be derived by evaluating the residue of the corresponding integrands at the closest poles to the contour, namely, the minimum pole on the right for large Fox's H-function arguments and the maximum pole on the left for small ones.

When $\mathscr{K}_N\gamma_{th} \to \infty$, then applying the residue method given in (Chergui *et al.*, 2016, Sec. IV), one can obtain

$$\mathscr{P}_{op} \approx 1 - \frac{\mathscr{K}_N}{\mathscr{C}}\text{Res}[\varepsilon(s),0] = 1 - \lim_{s\to 0} su(s) = 1 - \frac{\mathscr{K}_N}{\mathscr{C}}\prod_{k=1}^{N}\Gamma(\mu_k). \tag{A III-2}$$

2. Proof for Theorem 18

Revisiting (7.37) and using the Parseval's relation for Mellin transform (Debnath & Bhatta, 2014, eq. (8.3.23)), we have

$$\begin{aligned}\mathscr{I} &= \int_0^\infty \bar{F}_B(\gamma_0) f_E(\gamma_E) d\gamma_E \\ &= \frac{1}{2\pi j}\int_{\mathscr{L}_1} \mathscr{M}[\bar{F}_B(\gamma_0), 1-s]\mathscr{M}[f_E(\gamma_E), s] ds.\end{aligned} \tag{A III-3}$$

where $\mathscr{L}_1$ is the integration path from $\upsilon - j\infty$ to $\upsilon + j\infty$, and υ is a constant Debnath & Bhatta (2014) Then by introducing the definition of univariate Fox's H-function, $\mathscr{M}[\bar{F}_B(\gamma_0), 1-s]$ can be rewritten as

$$\begin{aligned}\mathscr{M}[\bar{F}_B(\gamma_0), 1-s] &= \int_0^{\infty} \gamma_E^{-s} F_B(\gamma_0) d\gamma_E \\ &\overset{(c)}{=} \frac{\mathscr{K}_{N_B}}{2\mathscr{C}_{N_B}\pi j} \int_{\mathscr{L}_2} \frac{\Gamma(\xi) \prod_{i=1}^{N_B} \Gamma(\mu_{B,i} + \frac{2}{\alpha_{B,i}}\xi)}{\Gamma(1+\xi)\mathscr{C}_{N_B}^{\xi}} \int_0^{\infty} \frac{\gamma_E^{-s}}{\gamma_0^{\xi}} d\gamma_E d\xi,\end{aligned} \tag{A III-4}$$

where step (c) is developed by interchanging the order of two integrals.

The inner integral in (A III-4) can be further written as

$$\begin{aligned}\int_0^{\infty} \gamma_E^{-s} \gamma_0^{-\xi} d\gamma_E &\overset{(d)}{=} \mathscr{W}^{-\xi} \int_0^{\infty} \frac{\gamma_E^{-s}}{\left(1 + \frac{R_s}{\mathscr{W}}\gamma_E\right)^{\xi}} d\gamma_E \\ &\overset{(e)}{=} \mathscr{W}^{-\xi} \mathscr{B}(1-s, \xi+s-1) \left(\frac{R_s}{\mathscr{W}}\right)^{s-1} \\ &\overset{(f)}{=} \mathscr{W}^{-\xi} \frac{\Gamma(1-s)\Gamma(\xi+s-1)}{\Gamma(\xi)} \left(\frac{R_s}{\mathscr{W}}\right)^{s-1},\end{aligned} \tag{A III-5}$$

where step (d) is developed by representing $\gamma_0 = R_s\gamma_E + \mathscr{W}$, step (e) is obtained from (Gradshteyn & Ryzhik, 2014, eq. (3.194.3)), and step (f) is further simplified in a closed-form by deploying the property $\mathscr{B}(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$ (Gradshteyn & Ryzhik, 2014, eq. (8.384.1)).

Next, plugging (A III-5) into (A III-4), yields the following result

$$\begin{aligned}\mathscr{M}[\bar{F}_B(\gamma_0), 1-s] &= \frac{\mathscr{K}_{N_B}}{2\mathscr{C}_{N_B}\pi j} \left(\frac{R_s}{\mathscr{W}}\right)^{s-1} \Gamma(1-s) \int_{\mathscr{L}} \frac{\Gamma(\xi+s-1) \prod_{i=1}^{N_B} \Gamma(\mu_{B,i} + \frac{2}{\alpha_{B,i}}\xi)}{\Gamma(1+\xi)(\lambda_B\mathscr{W})^{\xi}} d\xi \\ &\overset{(g)}{=} \frac{\mathscr{K}_{N_B}\Gamma(1-s)R_s^{s-1}}{\mathscr{C}_{N_B}\mathscr{W}^{s-1}} H_{1,N_B+1}^{N_B+1,0}\left[\mathscr{C}_{N_B}\mathscr{W} \middle| \begin{matrix}(1,1)\\ (s-1,1), \theta_1, \cdots, \theta_{N_B}\end{matrix}\right],\end{aligned} \tag{A III-6}$$

where step (g) is directly achieved from the definition of Fox's H-function.

Subsequently, substituting (A III-6) and $\mathscr{M}[f_E(\gamma_E),s]$ into (A III-3), where $\mathscr{M}[f_E(\gamma_E),s]$ is given by (Alhennawi *et al.*, 2016, eq. (5))

$$\mathscr{M}[f_E(\gamma_E),s] = \mathscr{C}_{N_E} \frac{\prod_{i=1}^{N_E} \Gamma\left(\mu_{E,i} - \frac{2}{\alpha_{E,i}} + \frac{2}{\alpha_{E,i}} s\right)}{\mathscr{C}_{N_E}^{s}}, \tag{A III-7}$$

results in the following result

$$\begin{aligned} \mathscr{I} = & -\frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}\mathscr{W}}{4\mathscr{C}_{N_B}R_s\pi^2} \int_{\mathscr{L}_1}\int_{\mathscr{L}_2} \frac{\Gamma(\xi+s-1)\prod_{i=1}^{N_B}\Gamma(\mu_{B,i}+\frac{2}{\alpha_{B,i}}\xi)}{\Gamma(1+\xi)(\mathscr{C}_{N_B}\mathscr{W})^{\xi}} \\ & \times \Gamma(1-s)\prod_{i=1}^{N_E}\Gamma\left(\mu_{E,i} - \frac{2}{\alpha_{E,i}} + \frac{2}{\alpha_{E,i}} s\right)\left(\frac{R_s}{\mathscr{C}_{N_E}\mathscr{W}}\right)^{s} d\xi\, ds. \end{aligned} \tag{A III-8}$$

Finally, plugging (A III-8) in (7.37) and subsequently applying the bivariate Fox's H-function (Mathai *et al.*, 2009a, eq. (2.57)), the proof is eventually achieved.

3. Proof for Asymptotic $\mathscr{P}_{out}$

In the case of $\bar{\gamma}_E \to \infty$, we have $\frac{R_s}{\mathscr{C}_{N_E}\mathscr{W}} \to \infty$. The bivariate Fox's H-function is evaluated at the highest poles on the left of $\mathscr{L}_1$, i.e., $s = 1-\xi$, by using the residue approach Chergui *et al.* (2016), therefore, it leads to the following result,

$$\begin{aligned} & \frac{1}{2\pi j}\int_{\mathscr{L}_1} \underbrace{\Gamma(\xi+s-1)\Gamma(1-s)\prod_{i=1}^{N_E}\Gamma\left(\mu_{E,i} - \frac{2}{\alpha_{E,i}} + \frac{2}{\alpha_{E,i}} s\right)\left(\frac{R_s}{\mathscr{C}_{N_E}\mathscr{W}}\right)^{s}}_{\psi(s)} ds \\ & \approx \mathrm{Res}[\psi(s), 1-\xi] \\ & = \lim_{s\to 1-\xi}(s+\xi-1)\psi(s) \\ & = \Gamma(\xi)\prod_{i=1}^{N_E}\Gamma\left(\mu_{E,i} - \frac{2}{\alpha_{E,i}}\xi\right)\left(\frac{R_s}{\mathscr{C}_{N_E}\mathscr{W}}\right)^{1-\xi}. \end{aligned} \tag{A III-9}$$

Therefore, we have

$$\mathscr{P}_{out} \approx 1 - \frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{2\pi\mathscr{C}_{N_B}\mathscr{C}_{N_E} j}\int_{\mathscr{L}_2} \underbrace{\frac{\Gamma(\xi)\prod_{i=1}^{N_E}\Gamma\left(\mu_{E,i}-\frac{2}{\alpha_{E,i}}\xi\right)\prod_{i=1}^{N_B}\Gamma\left(\mu_{B,i}+\frac{2}{\alpha_{B,i}}\xi\right)}{\Gamma(1+\xi)\left(\frac{\mathscr{C}_{N_B}R_s}{\mathscr{C}_{N_E}}\right)^{\xi}}}_{\tau(\xi)} d\xi, \qquad \text{(A III-10)}$$

continuation (A III-10) can be successively and asymptotically simplified as (10) by computing the highest pole on the right of the contour $\mathscr{L}_2$, namely $\xi = \frac{\alpha_{E,k}\mu_{E,k}}{2}$, where $\alpha_{E,k}\mu_{E,k} = \min(\alpha_{E,1}\mu_{E,1},\cdots,\alpha_{E,j}\mu_{E,j}), j = 1,\cdots,N_E$.

$$\mathscr{P}_{out} \approx 1 - \frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\mathscr{C}_{N_B}\mathscr{C}_{N_E}}\text{Res}\left[\tau(\xi), \frac{\alpha_{E,k}\mu_{E,k}}{2}\right], \qquad \text{(A III-11)}$$

then making some simple manipulations, the proof for (43) is achieved.

Following the same methodology, the proof for the case, $\bar{\gamma}_B \to \infty$, can be similarly achieved by first computing (A III-8) at the highest pole of $\mathscr{L}_2$ at $\xi = 1-s$, and subsequently evaluating the obtained result at the poles of $\mathscr{L}_1$, i.e., $s = 0$ and $s = \frac{\alpha_{B,k}\mu_{B,k}}{2}$, where $\alpha_{B,k}\mu_{B,k} = \min(\alpha_{B,1}\mu_{B,1},\cdots,\alpha_{B,i}\mu_{B,i}), i = 1,\cdots,N_B$, respectively.

When $\bar{\gamma}_E \to 0$, the asymptotic $\mathscr{P}_{out}$ is computed at the pole of $\mathscr{L}_1$, i.e., $s = 1$. For the case $\bar{\gamma}_B \to 0$, no pole exists on the right of the contour $\mathscr{L}_2$, $\mathscr{I}$ is directly equal to 1.

4. Proof for Theorem 16

For the ease of deriving the average secrecy capacity, the CDFs of γ_B and γ_E can be equivalently rewritten as follows by using (Bodenschatz, 1992, eq. (3.9))

$$F_B(\gamma_B) = \frac{\mathscr{K}_{N_B}}{\mathscr{C}_{N_B}} H_{1,N_B+1}^{N_B,1}\left[\mathscr{C}_{N_B}\gamma \,\middle|\, \begin{matrix}(1,1)\\ \phi_1,\cdots,\phi_{N_B},(0,1)\end{matrix}\right], \qquad \text{(A III-12a)}$$

$$F_E(\gamma_E) = \frac{\mathscr{K}_{N_E}}{\mathscr{C}_{N_E}} H_{1,N_E+1}^{N_E,1}\left[\mathscr{C}_{N_E}\gamma \middle| \begin{matrix}(1,1)\\ \theta_1,\cdots,\theta_{N_E},(0,1)\end{matrix}\right], \tag{A III-12b}$$

Recalling the result given in Lei *et al.* (2017a), the ASC given in (7.36) can be further mathematically expressed as

$$\bar{C}_s = \int_0^\infty \int_0^\infty C_s(\gamma_B,\gamma_E) f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_B d\gamma_E = \mathscr{I}_1 + \mathscr{I}_2 - \mathscr{I}_3, \tag{A III-13}$$

where $\mathscr{I}_1 = \int_0^\infty \log_2(1+\gamma_B) f_B(\gamma_B) F_E(\gamma_B) d\gamma_B$, $\mathscr{I}_2 = \int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) F_B(\gamma_E) d\gamma_E$, $\mathscr{I}_3 = \int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) d\gamma_E$.

Next, re-expressing the logarithm function in terms of the Meijer's *G*-function Prudnikov *et al.* (1990), and then using (Prudnikov *et al.*, 1990, Eq. (8.3.2.21))

$$\log_2(1+x) = \frac{1}{\ln 2} G_{2,2}^{1,2}\left[x \middle| \begin{matrix}(1,1)\\ (1,0)\end{matrix}\right], \quad H_{p,q}^{m,n}\left[x \middle| \begin{matrix}(a_p,1)\\ (b_q,1)\end{matrix}\right] = G_{p,q}^{m,n}\left[x \middle| \begin{matrix}(a_p)\\ (b_q)\end{matrix}\right].$$

$\mathscr{I}_1$ can be rewritten in (A III-14),

$$\begin{aligned}\mathscr{I}_1 = {} & \frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{\ln(2)\mathscr{C}_{N_E}} \int_0^\infty H_{2,2}^{1,2}\left[\gamma_B \middle| \begin{matrix}(1,1)(1,1))\\ (1,1),(0,1))\end{matrix}\right] H_{0,N_B}^{N_B,0}\left[\mathscr{C}_{N_B}\gamma_B \middle| \begin{matrix}-\\ \Phi_1,\cdots,\Phi_{N_B}\end{matrix}\right] \\ & \times H_{1,N_E+1}^{N_E,1}\left[\mathscr{C}_{N_E}\gamma_B \middle| \begin{matrix}(1,1)\\ \theta_1,\cdots,\theta_{N_E}\end{matrix}\right] d\gamma_B \\ = {} & \frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{2\pi j \ln(2)\mathscr{C}_{N_E}} \int_{\mathscr{L}_1} \frac{\prod_{l=1}^{N_E}\Gamma\left(\mu_{E,l} - \frac{2s}{\alpha_{E,l}}\right)\Gamma(s)}{\Gamma(1+s)\mathscr{C}_{N_E}^{-s}} \\ & \times \underbrace{\int_0^\infty \gamma_B^s H_{2,2}^{1,2}\left[\gamma_B \middle| \begin{matrix}(1,1),(1,1))\\ (1,1),(0,1)\end{matrix}\right] H_{0,N_B}^{N_B,0}\left[\mathscr{C}_{N_B}\gamma \middle| \begin{matrix}-\\ \Phi_1,\cdots,\Phi_{N_B}\end{matrix}\right] d\gamma_B}_{U} ds,\end{aligned} \tag{A III-14}$$

where $\mathscr{L}_1$ is a certain contour separating the poles of $\prod_{l=1}^{N_E}\Gamma(\mu_{E,l}-s)$ from the poles of $\Gamma(s)$. The inner integral U can be directly developed by using the Mellin transform for the product of two Fox's H-functions (Prudnikov *et al.*, 1990, eq. (2.25.1.1)) as follows

$$U=\mathscr{C}_{N_B}^{s+1}H_{2+N_B,2}^{1,2+N_B}\left[\frac{1}{\mathscr{C}_{N_B}}\middle|\begin{matrix}(1,1),(1,1),\omega_1,\cdots,\omega_{N_B}\\(1,1),(0,1)\end{matrix}\right], \tag{A III-15}$$

where $\omega_i=(1-\mu_{B,i}-\frac{2s}{\alpha_{B,i}},\frac{2}{\alpha_{B,i}})$, subsequently, rewriting (A III-15) in terms of the definition of Fox's H-function, then substituting the obtained result into (A III-14), leads to the result given in (A III-16),

$$\begin{aligned}\mathscr{I}_1=&-\frac{\mathscr{K}_{N_B}\mathscr{K}_{N_E}}{4\pi^2\ln(2)\mathscr{C}_{N_B}\mathscr{C}_{N_E}}\int_{\mathscr{L}_1}\int_{\mathscr{L}_2}\frac{\prod_{l=1}^{N_E}\Gamma\left(\mu_{E,l}-\frac{2s}{\alpha_{E,l}}\right)\Gamma(s)\Gamma(1-t)\Gamma^2(t)}{\Gamma(1+s)\Gamma(1+t)\mathscr{C}_{N_B}^t}\left(\frac{\mathscr{C}_{N_E}}{\mathscr{C}_{N_B}}\right)^s\\&\times\prod_{i=1}^{N_B}\Gamma\left(m_{B,i}+\frac{2s}{\alpha_{B,i}}+\frac{2t}{\alpha_{B,i}}\right)dtds,\end{aligned} \tag{A III-16}$$

where $\mathscr{L}_2$ is another contour, next recognizing the definition of bivariate Fox's H-functions Mathai *et al.* (2009a), the proof for $\mathscr{I}_1$ is accomplished.

Similarly, following the same methodology, the proof for $\mathscr{I}_2$ is achieved.

With the help of (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), the proof for $\mathscr{I}_3$ can be similarly obtained.

APPENDIX IV

PROOFS FOR CHAPTER 8

1. Derivation of $f_{\frac{g_k}{r_k^{\upsilon}}}(z)$

Setting $Z = \frac{g_k}{r_k^{\upsilon}}$, the PDF of Z can be assessed by the ratio of g_k and r_k^{υ}, given by the following form

$$f_{\frac{g_k}{r_k^{\upsilon}}}(z) = \int_0^{\infty} y f_{g_k}(yz) f_{r_k^{\upsilon}}(y) dy \overset{(b)}{=} \frac{\delta A_k^k \varepsilon_k}{\Gamma(k)} \int_0^{\infty} y^{k\delta} \exp(-A_k y^{\delta}) H_{0,1}^{1,0}\left[\theta_k zy \,\middle|\, \begin{matrix} - \\ (\mu_k - \frac{2}{\alpha_k}, \frac{2}{\alpha_k}) \end{matrix}\right] dy, \tag{A IV-1}$$

where $f_{r_k^{\upsilon}}(y) = \exp(-A_k y^{\delta}) \frac{\delta (A_k y^{\delta})^k}{y\Gamma(k)}$, $A_k = \pi\lambda_b$ (Liu *et al.*, 2014, eq. (5)), (b) is developed by substituting (8.2).

Since the exponential function can be expressed in terms of Fox's H-function (Jeong *et al.*, 2014, eq. (17)), given as

$$\exp(-A_k y^{\delta}) = \frac{1}{\delta} H_{0,1}^{1,0}\left[A_k^{\frac{1}{\delta}} y \,\middle|\, \begin{matrix} - \\ (0, \frac{1}{\delta}) \end{matrix}\right], \tag{A IV-2}$$

subsequently, substituting (A IV-2) into (A IV-1) and using the Mellin transform of the product of two Fox's H-function (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), the proof is concluded.

2. Derivation of $F_{\frac{g_k}{r_k^{\upsilon}}}(z)$

Essentially, $F_{\frac{g_k}{r_k^{\upsilon}}}(z)$ can be mathematically expressed as

$$\begin{aligned} F_{\frac{g_k}{r_k^{\upsilon}}}(z) &= \int_0^{\infty} F_{g_k}(yz) f_{r_k^{\upsilon}}(y) dy \\ &= 1 - \frac{\delta \varepsilon_k A_k^k}{\theta_k \Gamma(k)} \int_0^{\infty} y^{k\delta - 1} \exp(-A_k y^{\delta}) H_{1,2}^{2,0}\left[A_k^{\frac{1}{\delta}} y \,\middle|\, \begin{matrix} (1,1) \\ (0,1), (\mu_k, \frac{2}{\alpha_k}) \end{matrix}\right] dy, \end{aligned} \tag{A IV-3}$$

by using (A IV-2) and with the aid of (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), the proof is finally achieved.

3. Proof of Lemma 2

The intensity function of $\Psi = \{r_k^v\}$ can be derived from $\mathbb{E}\{\Psi[0,x)\} = \lambda_b c_d x^\delta$ by utilizing the mapping theorem (Haenggi, 2008b, Corollary 2.a), i.e., $\lambda_\Psi = \lambda_b c_d \delta x^{\delta-1}$.

The intensity of Ξ_k is obtained by applying the displacement theorem Haenggi, M. (2012) as follows

$$\begin{aligned}\lambda_{\Xi_k} &= \int_0^\infty \lambda_\Psi \rho(x,y)dx = \int_0^\infty \lambda_\Psi \frac{x}{y^2} f_{g_k}(x/y)dx \\ &= \int_0^\infty \lambda_b c_d \delta \frac{x^\delta}{y^2} f_{g_k}(x/y)dx \overset{(c)}{=} \lambda_b c_d \delta y^{\delta-1} \underbrace{\int_0^\infty z^\delta f_{g_k}(z)dz}_{U_4},\end{aligned} \tag{A IV-4}$$

where (c) is obtained by changing the variable $z = x/y$. The integral in (A IV-4) is solved as

$$U_4 = \int_0^\infty \frac{\alpha_k z^{\frac{\alpha_k\mu_k}{2}+\delta-1}}{2\Omega_k^{\frac{\alpha_k\mu_k}{2}}\Gamma(\mu_k)} \exp\left(-\left(\frac{z}{\Omega_k}\right)^{\frac{\alpha_k}{2}}\right)dz \overset{(d)}{=} \frac{\Gamma(\mu_k+\frac{2\delta}{\alpha_k})\Omega_k^\delta}{\Gamma(\mu_k)}, \tag{A IV-5}$$

where (d) holds by using (Gradshteyn & Ryzhik, 2014, eq. (3.381.10)). The proof is eventually concluded by substituting (A IV-5) into (A IV-4).

4. Proof of Lemma 3

By using (Tolossa *et al.*, 2017, Lemma 2), we have

$$\begin{aligned}F_{\xi_k}(x) &= \mathscr{P}r(\xi_k < x) = 1 - \mathscr{P}r(\Xi[0,x] < k) = 1 - \sum_{n=0}^{k-1} \exp\left(-\int_0^x \lambda_{\Xi_k}(y)dy\right) \frac{\left(\int_0^x \lambda_{\Xi_k}(y)dy\right)}{n!} \\ &= 1 - \sum_{n=0}^{k-1} \exp(-A_{b1}x^\delta)\frac{(A_{b1}x^\delta)^n}{n!} = \frac{\gamma\left(k, A_{b1}x^\delta\right)}{\Gamma(k)}.\end{aligned} \tag{A IV-6}$$

When taking the derivative of (A IV-6), all terms in the sum are canceled out but the one for $n-1$. The PDF of ξ_k becomes

$$f_{\xi_k}(x) = \exp\left(-A_{b1}x^{\delta}\right)\frac{\delta(A_{b1}x^{\delta})^k}{x\Gamma(k)}. \tag{A IV-7}$$

Therefore, the composite channel gain for the k-th best user can be termed as

$$F_{\frac{1}{\xi_k}} = \mathscr{P}r\left(\frac{1}{\xi_k} < z\right) = 1 - F_{\xi_k}\left(\frac{1}{z}\right) = 1 - \frac{\gamma\left(k, A_{b1}z^{-\delta}\right)}{\Gamma(k)} = \frac{\Gamma\left(k, A_{b1}z^{-\delta}\right)}{\Gamma(k)}. \tag{A IV-8}$$

Herein, the last step is derived from (Gradshteyn & Ryzhik, 2014, eq. (8.356.3)). By taking the derivative of $F_{\frac{1}{\xi_k}}(z)$ in terms of z, the PDF of $\frac{1}{\xi_k}$ is directly obtained.

5. Derivation of $\mathscr{P}_{nz,NN}$ in (8.19)

Inspired by Lemma 1, $\mathscr{P}_{nz,NN}$ can be essentially derived as follows

$$\begin{aligned}\mathscr{P}_{nz,NN} &= \int_0^{\infty} F_{\frac{g_e}{r_e^{\upsilon}}}(\varpi y) f_{\frac{g_k}{r_k^{\upsilon}}}(y)\, dy \\ &= 1 - \frac{\varepsilon_k \varepsilon_e}{\theta_e A_k^{\frac{1}{\delta}}\Gamma(k)} \int_0^{\infty} H_{1,1}^{1,1}\left[\frac{\theta_k}{A_k^{\frac{1}{\delta}}} y \middle| \begin{matrix}(1-k-\frac{1}{\delta}, \frac{1}{\delta}) \\ (\mu_k - \frac{2}{\alpha_k}, \frac{2}{\alpha_k})\end{matrix}\right] H_{2,2}^{2,1}\left[\frac{\theta_e}{A_e^{\frac{1}{\delta}}}\varpi y \middle| \begin{matrix}(0, \frac{1}{\delta}), (1,1) \\ (0,1), (\mu_e, \frac{2}{\alpha_e})\end{matrix}\right] dy,\end{aligned} \tag{A IV-9}$$

with the help of (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), the proof is accomplished.

6. Derivation of $\mathscr{P}_{nz,NB}$ in (8.24)

Thanks to the CDF of $\frac{g_k}{r_k^{\upsilon}}$ and PDF of ξ_e, respectively given in (8.4b) and (A IV-7), the expression $\mathscr{P}_{nz,NB}$ can be easily stated as

$$\begin{aligned}\mathscr{P}_{nz,NB} &= 1 - \int_0^{\infty} F_{\frac{g_k}{r_k^{\upsilon}}}\left(\frac{1}{\varpi y}\right) f_{\xi_e}(y) dy \\ &= \frac{2\delta A_{e1}}{\alpha_k \Gamma(\mu_k)\Gamma(k)} \int_0^{\infty} y^{\delta-1}\exp(-A_{e1}y^{\delta}) H_{2,2}^{2,1}\left[\frac{\varpi_k}{\varpi A_k^{\frac{1}{\delta}} y} \middle| \begin{matrix}(1-k, \frac{1}{\delta}), (1,1) \\ (0,1), (\mu_k, \frac{2}{\alpha_k})\end{matrix}\right] dy.\end{aligned} \tag{A IV-10}$$

By using (A IV-2) and with the assistance of the property of Fox's H-function (Prudnikov *et al.*, 1990, eq. (8.3.2.7)),

$$H_{2,2}^{2,1}\left[\frac{\varpi_k}{\varpi A_k^{\frac{1}{\delta}} y}\middle|\begin{matrix}(1-k,\frac{1}{\delta}),(1,1)\\(0,1),(\mu_k,\frac{2}{\alpha_k})\end{matrix}\right]=H_{2,2}^{1,2}\left[\frac{\varpi A_k^{\frac{1}{\delta}} y}{\varpi_k}\middle|\begin{matrix}(1,1),(1-\mu_k,\frac{2}{\alpha_k})\\(k,\frac{1}{\delta}),(0,1)\end{matrix}\right]. \tag{A IV-11}$$

$\mathscr{P}_{nz,NB}$ can be further developed as

$$\begin{aligned}\mathscr{P}_{nz,NB}=&\frac{2A_{e1}}{\alpha_k\Gamma(\mu_k)\Gamma(k)}\int_0^\infty y^{\delta-1}H_{0,1}^{1,0}\left[A_{e1}^{\frac{1}{\delta}}y\middle|\begin{matrix}-\\(0,\frac{1}{\delta})\end{matrix}\right]\\&\times H_{2,2}^{1,2}\left[\varpi\Omega_k A_k^{\frac{1}{\delta}}y\middle|\begin{matrix}(1-k,\frac{1}{\delta}),(1,\frac{2}{\alpha_k})\\(\mu_k,\frac{2}{\alpha_k}),(0,\frac{2}{\alpha_k})\end{matrix}\right]dy,\end{aligned} \tag{A IV-12}$$

afterwards, performing the Mellin transform of the product of two Fox's H-functions (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), the proof is eventually obtained.

7. Derivation of $\mathscr{P}_{nz,BN}$ in (8.25)

The $\mathscr{P}_{nz,BN}$ in (8.18) can be tracked from the PDF of ξ_k and the CDF of $\frac{g_e}{r_e^v}$, $\mathscr{P}_{nz,4}$ is given by

$$\begin{aligned}\mathscr{P}_{nz,BN}&=\int_0^\infty F_{\frac{g_e}{r_e^v}}\left(\frac{\varpi}{y}\right)f_{\xi_k}(y)dy\\&=1-\frac{\varepsilon_e\delta A_{b1}^{\frac{1}{\delta}}}{\theta_e\Gamma(k)}\int_0^\infty y^{k\delta-1}\exp(-A_{b1}y^\delta)H_{2,2}^{2,1}\left[\frac{\theta_e\varpi}{A_e^{\frac{1}{\delta}}y}\middle|\begin{matrix}(0,\frac{1}{\delta}),(1,1)\\(0,1),(\mu_e,\frac{2}{\alpha_e})\end{matrix}\right]dy.\end{aligned} \tag{A IV-13}$$

Subsequently, following the similar steps as (A IV-10-A IV-12), the proof is easily proved.

8. Derivation of Proposition (11)

As the very beginning, the logarithm function and exponential function can be alternatively rewritten in terms of the Fox's H-function (Mathai & Saxena, 1978, eq. (1.7.2)) and (Prudnikov

et al., 1990, eq. (8.4.6.5))

$$\log_2(1+x) = \frac{1}{\ln 2} H_{2,2}^{1,2}\left[x \left| \begin{matrix} (1,1),(1,1) \\ (1,1),(0,1) \end{matrix} \right. \right], \tag{A IV-14}$$

$$\exp(-x) = H_{0,1}^{1,0}\left[x \left| \begin{matrix} - \\ (0,1) \end{matrix} \right. \right]. \tag{A IV-15}$$

$$\begin{aligned} R_{N,k}^{M} &= \mathbb{E}_{\frac{g_k}{r_k^{\upsilon}}}\left[\log_2\left(1 + \frac{\eta_k g_k}{r_k^{\upsilon}} \right) \right] \\ &= \frac{\varepsilon_k}{A_k^{\frac{1}{\delta}} \Gamma(k) \ln 2} \int_0^{\infty} H_{2,2}^{1,2}\left[\eta_k y \left| \begin{matrix} (1,1),(1,1) \\ (1,1),(0,1) \end{matrix} \right. \right] H_{1,1}^{1,1}\left[\frac{\theta_k y}{A_k^{\frac{1}{\delta}}} \left| \begin{matrix} (1-k-\frac{1}{\delta},\frac{1}{\delta}) \\ (\mu_k - \frac{2}{\alpha_k},\frac{2}{\alpha_k}) \end{matrix} \right. \right] dy. \end{aligned} \tag{A IV-16}$$

Next, applying the Mellin transform of the product of two Fox's H-function (Prudnikov *et al.*, 1990, eq. (2.25.1.1)), the proof is accomplished.

Using (Mathai & Saxena, 1978, eq. (1.2.4)), the PDF of ξ_k in (A IV-7) can be re-expressed in terms of Fox's H-function,

$$f_{\xi_k}(x) = \frac{\delta}{x\Gamma(k)} H_{0,1}^{1,0}\left[A_{b1} x^{\delta} \left| \begin{matrix} - \\ (k,1) \end{matrix} \right. \right], \tag{A IV-17}$$

subsequently, using (Mathai & Saxena, 1978, eq. (1.2.2)) of $\log_2(1+\frac{1}{x})$ and plugging (A IV-17), yields

$$\begin{aligned} R_{B,k}^{M} &= \mathbb{E}_{\xi_k}\left[\log_2\left(1 + \frac{\eta_k}{\xi_k} \right) \right] \\ &= \frac{\delta}{\Gamma(k)\ln 2} \int_0^{\infty} y^{-1} H_{2,2}^{1,2}\left[\frac{y}{\eta_k} \left| \begin{matrix} (1,1),(1,1) \\ (1,1),(0,1) \end{matrix} \right. \right] H_{0,1}^{1,0}\left[A_{b1} y^{\delta} \left| \begin{matrix} - \\ (k,1) \end{matrix} \right. \right] dy, \end{aligned} \tag{A IV-18}$$

next, using (Prudnikov *et al.*, 1990, eq. (2.25.1.1)) and (Mathai & Saxena, 1978, eq. (1.7.1)), the proof is achieved.

APPENDIX V

SECRECY ANALYSIS OF A MIMO FULL-DUPLEX ACTIVE EAVESDROPPER WITH CHANNEL ESTIMATION ERRORS

Long Kong[1], Jiguang He[2], Georges Kaddoum[1], Satyanarayana Vuppala[3], and Lin Wang[4]

[1]Département de Génie électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3
[2]Centre for Wireless Communications, FI-90014, University of Oulu, Oulu, Finland
[3]IDCOM, school of Engineering, University of Edinburgh, Edinburgh, United Kingdom
[4]Department of Communication Engineering, Xiamen University, Xiamen, P.R. China

Paper published in *IEEE 84th Vehicular Technology Conference*, September 2016.

1. Abstract

In this paper, we investigate the secrecy performance of the multiple-input multiple-output (MIMO) wiretap channels in the presence of an active full-duplex eavesdropper with consideration of channel estimation error at the legitimate destination and eavesdropper. For this purpose, the probability density functions (PDFs) and cumulative density functions (CDFs) of the receive signal-to-interference-plus-noise ratio (SINR) at the destination and eavesdropper are given by conducting the singular value decomposition (SVD) on the estimated channel coefficient matrices. Consequently, the closed-form expressions for the probability of positive secrecy capacity and secrecy outage probability over Rayleigh fading channels are derived. Finally, the Monte-Carlo simulation results are presented to validate the accuracy of our theoretical analysis.

Keywords: Physical layer security, channel estimation error, the MIMO full-duplex active eavesdropper.

2. Introduction

Due to the broadcast nature of wireless channels, security issues are increasingly becoming one of the top critical concerns of wireless network. Currently, the traditional cryptography

technique widely used in the upper-layer of wireless networks faces big challenges because of the high computational complexity of the communication devices. Fortunately, unlike the traditional methods, a complement or alternative appealing approach termed as physical layer security was emerged to achieve secure wireless transmission, which is based on Shannon theory Shannon (1949) using the physical characteristics (i.e. noise, fading, interference) of wireless channels. The main philosophy of physical layer security is to achieve perfect secrecy capacity from the information-theoretic perspective, which is defined as the maximization of wireless transmission rate while achieving perfect secure transmission Bloch & Barros (2011). In other words, it can be further explained as that eavesdroppers can not do better than the legitimate destinations Saad, W., Zhou, X., Debbah, M. & Poor, H. (2015). Against this background, some promising techniques, such as multiple antennas, cooperative jamming/relay Allen, T. & Al-Dhahir, N. (2015); Atallah, M., Kaddoum, G. & Kong, L. (2015); Bloch & Barros (2011); Saad *et al.* (2015); Yan, S., Yang, N., Malaney, R. & Yuan, J. (2014), are exploited to degrade the capability of either active attacker or passive eavesdroppers so as to ease the information leakage.

Multiple antenna technique, as an effective approach, is widely used toward improving the secrecy rate. The literature using MIMO technique in the filed of physical layer security demonstrated its capability of boosting secrecy performance Ahn, K. S., Choi, S.-W. & Ahn, J.-M. (2015); Khisti, A. & Wornell, G. W. (2010b); Mukherjee, A. & Swindlehurst, A. (2011); Oggier, F. & Hassibi, B. (2015); Shafiee, S., Liu, N. & Ulukus, S. (2009); Yan *et al.* (2014). In particular, the secrecy performance of single-input multiple-output (SIMO) Ahn *et al.* (2015), multiple-input single-output (MISO) Khisti & Wornell (2010a) and multiple-input multiple-output (MIMO) Khisti & Wornell (2010b) were widely studied from the information-theoretic viewpoint. Shafiee. *et. al* investigated the existence of a computable expression for the secrecy capacity of a 2-2-1 MIMO wiretap channel Shafiee *et al.* (2009). Yan. *et. al* investigated the classical three-player MIMO wiretap scenario that Alice firstly selects two strongest transmitter antennas from its multiple antenna set based on the channel gain for the sake of maximizing the instantaneous signal-to-noise ratio (SNR) and then performs Alamouti coding over the se-

lected antennas, afterwards, the closed-form expression of secrecy outage probability for the proposed scheme was derived Yan *et al.* (2014). In Mukherjee & Swindlehurst (2011), an optimal jamming policy for a full-duplex active eavesdropper to minimize the secrecy rate of the Alice-Bob-Eve MIMO wiretap channel was examined. The authors of Ahn *et al.* (2015) analyzed the secrecy performance of a SIMO wiretap channel with channel estimation errors available at the legitimate receiver and eavesdropper, its conclusion suggests that there exists error floor of secrecy outage probability caused by the imperfect channel estimation.

Motivated by these studies, it is so far that there is no previous work that studied the secrecy performance of a 2-2-2 MIMO wiretap channel with consideration of channel estimation error whilst in the presence of an active full-duplex eavesdroppers. To this end, the contribution of this paper lies in the investigation of the secrecy performance of the 2-2-2 MIMO wiretap channel, including the probability of positive secrecy capacity and secrecy outage probability, over Rayleigh fading in the presence of an active full-duplex eavesdropper with channel estimation errors at the legitimate receiver and eavesdropper side. First, the probability density functions (PDFs) and cumulative density functions (CDFs) of the signal-to-interference-plus-noise ratios (SINRs) of Bob's and Eve's received signals are given. Second, the closed-form expressions for the secrecy metrics are derived, and the Monte-Carlo simulation are presented to examine our theoretical analysis.

The remainder of this paper is organized as follows. System model and problem formulation are outlined in Section II. In the Section III, secrecy performance, including the probability of positive secrecy capacity and secrecy outage probability, are derived with closed-form expressions, followed by the comparison of theoretical analysis and numerical simulations given in Section IV. Finally, concluding remarks are given in Section V.

Notations: In this paper, matrices and vectors are separately presented by boldfaced uppercase (e.g., $\mathbf{X}$) and lowercase (e.g., $\mathbf{x}$) letters. Moreover, we use $\mathbf{X}^H$ to denote the Hermitian transpose of the matrix $\mathbf{X}$, $\mathrm{Tr}(\cdot)$ to the trace operator, $\mathbf{E}(\cdot)$ to the expectation operator, $\mathbf{I}_m$ the identity

matrix of m dimension, $\mathbf{y} \sim \mathscr{CN}(\mu,\sigma^2\mathbf{I})$ to denote that y is the complex Gaussian random variable, having a μ-mean and σ^2-variance.

3. System Model and Problem Formulation

3.1 System Model

The Alice-Bob-Eve classic model shown in Fig. V-1 is used here to illustrate a wireless network with a potential active eavesdropper, where all the users are equipped with 2 antennas. In such a wiretap channel model, the transmitter Alice (A) wishes to send secret messages to the intended receiver Bob (B) in the presence of an active eavesdropper Eve (E); the link between Alice and Bob is called the main channel, whereas the one between Alice and Eve is named as the wiretap channel, and the one between Eve and Bob is termed as interference channel. It is assumed that all links are independent and undergoing quasi-static Rayleigh fading. The fading coefficients of the links $i \rightarrow j$ are denoted as $\mathbf{H}_{ij}$, $i, j \in \{A, B, E\}$. In addition, assuming Eve operates in the full-duplex mode, it means that she can listen to data transmission of main channel whilst transmitting jamming signals to Bob. Additionally, it is assumed that Bob and Eve have imperfect channel state information (CSI) of their links, and Alice and Bob have no knowledge of the CSI of the wiretap links.

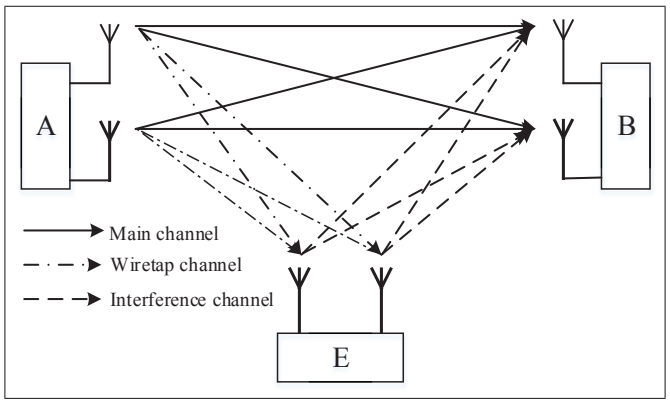


Figure-A V-1 System model

Then, the received signal at Bob and Eve can be expressed as

$$\mathbf{r}_B = \mathbf{H}_{\mathrm{AB}}\mathbf{x}_A + \mathbf{H}_{\mathrm{EB}}\mathbf{x}_E + \mathbf{n}_B, \tag{A V-1}$$

$$\mathbf{r}_E = \mathbf{H}_{\mathrm{AE}}\mathbf{x}_A + \mathbf{H}_{\mathrm{EE}}\mathbf{x}_E + \mathbf{n}_E, \tag{A V-2}$$

where $\mathbf{x}_A$ and $\mathbf{x}_E$ are the 2×1 transmit signal vector from Alice and jamming signal vector from Eve, respectively. Alice's transmit power is assumed to be fixed to $\mathrm{Tr}\{E[\,\mathbf{x}_A\mathbf{x}_A^H]\} = P_A$. Likewise, Eve's jamming power is subject to $\mathrm{Tr}\{E[\mathbf{x}_E\mathbf{x}_E^H]\} = P_E$. Each entry of $\mathbf{H}_{ij}$ follows independent identically distributed (i.i.d.) Gaussian distribution with zero mean and unit variance, denoted by $\mathbf{H}_{ij}(m,n) \sim \mathscr{CN}(0,1)$ for $m,n \in \{1,2\}$. $\mathbf{n}_B$ and $\mathbf{n}_E$ are the zero mean additive white Gaussian noise (AWGN) distributed with $\mathscr{CN}(0,\sigma_B^2\mathbf{I})$ and $\mathscr{CN}(0,\sigma_E^2\mathbf{I})$, respectively.

3.2 Problem Formulation

Due to the characteristic of wireless channel, a practical imperfect channel estimator is frequently exploited at the legitimate receivers. The following model is broadly used throughout this paper for the estimated channel $\hat{\mathbf{H}}_{ij}$ Ahn *et al.* (2015),

$$\mathbf{H}_{ij} = \sqrt{1-\varepsilon_{ij}^2}\hat{\mathbf{H}}_{ij} + \varepsilon_{ij}\mathbf{V}_{ij}, \tag{A V-3}$$

where each entry of $\mathbf{V}_{ij}$ follows $\mathscr{CN}(0,\mathbf{I})$, $\mathbf{V}_{ij}$ is independent of $\mathbf{H}_{ij}$, and $\varepsilon_{ij} \in [0,1]$ is used to measure the accuracy of the channel estimation.

Setting $\mathbf{H}_{\mathrm{B}} = \hat{\mathbf{H}}_{\mathrm{AB}}\hat{\mathbf{H}}_{\mathrm{AB}}^H$, $\mathbf{H}_{\mathrm{B}}$ can be decomposed as $\mathbf{H}_{\mathrm{B}} = \mathbf{W}_{\mathrm{B}}\Lambda\mathbf{W}_{\mathrm{B}}^H$ by using the singular value decomposition (SVD), where $\Lambda = \mathrm{diag}(\lambda_1,\lambda_2)$ and $\lambda_1 \geq \lambda_2 \geq 0$. $\mathbf{W}_{\mathrm{B}}$ is an unitary matrix, i.e., $\mathbf{W}_{\mathrm{B}}\mathbf{W}_{\mathrm{B}}^H = \mathbf{I}$. Based on the above description, we choose $\mathbf{W}_B$ as the combiner matrix at user B. Similarly, $\mathbf{W}_E$ can be constructed in the same way as $\mathbf{W}_B$, and then is used as the combining matrix at user E.

Consequently, while taking consideration of channel estimation error, the combined signals at Bob and Eve are given by

$$\begin{aligned}\mathbf{Y}_B &= \mathbf{W}_{\mathrm{B}}^H \mathbf{r}_B \\ &= \sqrt{1-\varepsilon_{AB}^2}\mathbf{Y}_{\mathrm{B}}^H \hat{\mathbf{H}}_{\mathrm{AB}}\mathbf{x}_A + \varepsilon_{AB}\mathbf{W}_{\mathrm{B}}^H \mathbf{V}_{\mathrm{AB}}\mathbf{x}_A + \mathbf{W}_{\mathrm{B}}^H\left(\mathbf{H}_{\mathrm{BE}}\mathbf{x}_E + \mathbf{n}_B\right),\end{aligned} \tag{A V-4}$$

$$\begin{aligned}\mathbf{Y}_E &= \mathbf{W}_{\mathrm{E}}^H \mathbf{r}_E \\ &= \sqrt{1-\varepsilon_{AE}^2}\mathbf{W}_{\mathrm{E}}^H \hat{\mathbf{H}}_{\mathrm{AE}}\mathbf{x}_A + \varepsilon_{AE}\mathbf{W}_{\mathrm{E}}^H \mathbf{V}_{\mathrm{AE}}\mathbf{x}_A + \mathbf{W}_{\mathrm{E}}^H\left(\mathbf{H}_{\mathrm{EE}}\mathbf{x}_E + \mathbf{n}_E\right).\end{aligned} \tag{A V-5}$$

Therefore, the average SINR of the combined signal at Bob's side γ_B is given by

$$\gamma_{\mathrm{B}} = \Omega_B \mathrm{Tr}(\mathbf{W}_B^H \hat{\mathbf{H}}_{\mathrm{AB}} \hat{\mathbf{H}}_{\mathrm{AB}}^H \mathbf{W}_B), \tag{A V-6}$$

where $\Omega_B = \frac{P_A(1-\varepsilon_{AB}^2)}{2\varepsilon_{AB}^2 P_A + \sigma_B^2 + 2P_E} = \frac{\Phi_B(1-\varepsilon_M^2)}{2\varepsilon_M^2\Phi_B + 1 + 2\Phi_J}$. Herein, $\Phi_B = P_A/\sigma_B^2$, $\Phi_J = P_E/\sigma_B^2$. For convenience, $\varepsilon_{AB}^2 = \varepsilon_M^2$.

Obviously, the denominator is constant while the numerator is equal to the sum of the eigenvalues of the Wishart matrix $\hat{\mathbf{H}}_{\mathrm{AB}}\hat{\mathbf{H}}_{\mathrm{AB}}^H$. Based on the random matrix theory, the joint PDF of the ordered eigenvalues of $\mathbf{H}_{\mathrm{B}}$ can be expressed as Telatar, I. E. et al. (1999)

$$p(\lambda_1, \lambda_2) = (\lambda_2 - \lambda_1)^2 e^{-\lambda_1 - \lambda_2}. \tag{A V-7}$$

Let $\lambda = \lambda_1 + \lambda_2$, then $\gamma_B = \Omega_B \lambda$. The CDF of γ_B can be expressed as

$$\begin{aligned}F_{\gamma_B}(\gamma_B) &= Pr\left(\Omega_B\left(\lambda_1 + \lambda_2\right) \le \gamma_B\right) \\ &= \int_0^{\frac{\gamma_B}{2\Omega_B}} \int_{\lambda_2}^{\frac{\gamma_B}{\Omega_B} - \lambda_2} p(\lambda_1, \lambda_2) d\lambda_1 d\lambda_2 \\ &= 1 - \left[\left(\frac{\gamma_B}{\Omega_B}\right)^3 + 3\left(\frac{\gamma_B}{\Omega_B}\right)^2 + 6\left(\frac{\gamma_B}{\Omega_B}\right) + 6\right]\frac{e^{-\frac{\gamma_B}{\Omega_B}}}{6}.\end{aligned} \tag{A V-8}$$

Differentiating (A V-8) with regard to γ_B, the PDF of γ_B is established as follows

$$f_{\gamma_B}(\gamma_B) = \frac{dF_{\gamma_B}(\gamma_B)}{d\gamma_B} = \frac{\gamma_B^3}{6\Omega_B^4} e^{-\frac{\gamma_B}{\Omega_B}}. \tag{A V-9}$$

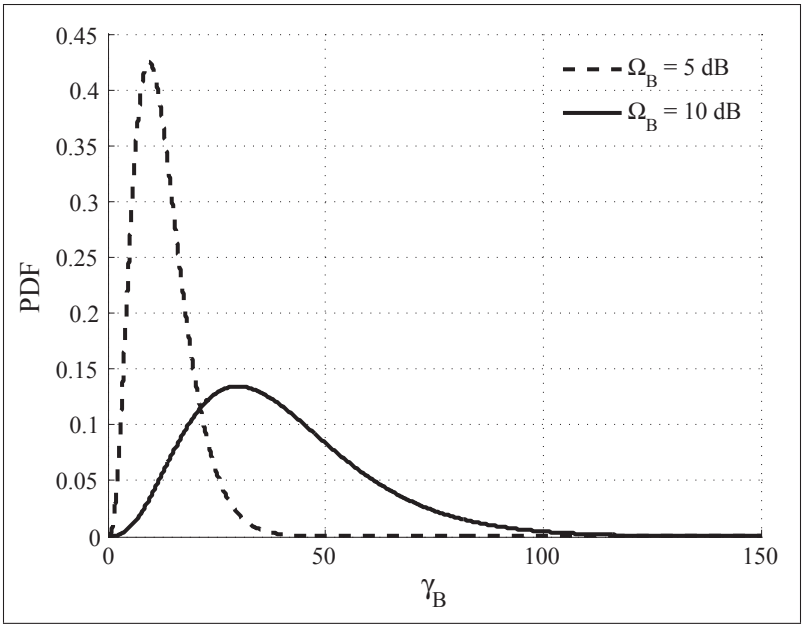


Figure-A V-2 The PDFs of γ_B when Ω_B are 5 dB and 10 dB, respectively.

Fig. V-2 shows the PDFs of γ_B with respect to different values of Φ_B.

It is assumed that perfect self-interference cancellation can be performed at the Eve's side. Likewise, we have the received average SINR at Eve

$$\gamma_{\mathrm{E}} = \Omega_E Tr(\mathbf{W}_E^H \hat{\mathbf{H}}_{\mathrm{AB}} \hat{\mathbf{H}}_{\mathrm{AB}}^H \mathbf{W}_E), \tag{A V-10}$$

where $\Omega_E = \frac{(1-\varepsilon_{AE}^2)P_A}{2\varepsilon_{AE}^2 P_A + \sigma_E^2} = \frac{(1-\varepsilon_W^2)\Phi_E}{2\varepsilon_W^2 \Phi_E + 1}$, $\Phi_E = P_A/\sigma_E^2$, and $\varepsilon_{AE}^2 = \varepsilon_W^2$.

The CDF and PDF of γ_E are

$$F_{\gamma_E}(\gamma_E) = 1 - \left[(\frac{\gamma_E}{\Omega_E})^3 + 3(\frac{\gamma_E}{\Omega_E})^2 + 6(\frac{\gamma_E}{\Omega_E}) + 6 \right] \frac{e^{-\frac{\gamma_E}{\Omega_E}}}{6}, \tag{A V-11}$$

and

$$f_{\gamma_E}(\gamma_E) = \frac{\gamma_E^3}{6\Omega_E^4} e^{-\frac{\gamma_E}{\Omega_E}}, \tag{A V-12}$$

respectively.

4. Secrecy Performance Analysis

4.1 Probability of Positive Secrecy Capacity

According to Bloch & Barros (2011), the secrecy capacity for the MIMO wiretap channel over Rayleigh fading is defined as the difference between the main channel capacity $C_M = \log_2(1+\gamma_B)$ and the wiretap channel capacity $C_W = \log_2(1+\gamma_E)$ as the following form,

$$C_s = \begin{cases} C_M - C_W, & \gamma_B > \gamma_E \\ 0, & \text{otherwise.} \end{cases} \tag{A V-13}$$

Therefore, the probability of positive secrecy capacity refers to the event that the secrecy capacity can be achieved, i.e. $Pr(C_s > 0)$, thus with regard to its definition, (A V-13) can be further rewritten as follows,

$$\begin{aligned} Pr(C_s > 0) &= Pr(\gamma_B > \gamma_E) \\ &= \int_0^\infty \int_0^{\gamma_B} f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_E d\gamma_B \\ &= \int_0^\infty f_{\gamma_B}(\gamma_B) F_{\gamma_E}(\gamma_B) d\gamma_B. \end{aligned} \tag{A V-14}$$

Substituting (A V-9) and (A V-11) into (A V-14), we use the equation (A V-15) (Gradshteyn & Ryzhik, 2014, Eq. (3.351.3)),

$$\int_0^\infty x^n e^{-\mu x} dx = \begin{cases} n!\mu^{-n-1}, & \text{if n = 0,1,2,}\cdots, \mu > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{A V-15}$$

then we have the closed-form expression for the probability of positive secrecy capacity in (A V-16)

$$\begin{aligned} Pr(C_s>0) =& 1-\frac{1}{\Omega_B^4\Omega_E^3}\left[20(\frac{1}{\Omega_B}+\frac{1}{\Omega_E})^{-7}+10\Omega_E(\frac{1}{\Omega_B}+\frac{1}{\Omega_E})^{-6}\right. \\ &\left.+\Omega_E^2(\frac{1}{\Omega_B}+\frac{1}{\Omega_E})^{-5}+\Omega_E^3(\frac{1}{\Omega_B}+\frac{1}{\Omega_E})^{-4}\right]. \end{aligned} \tag{A V-16}$$

4.2 Secrecy Outage Probability

The outage probability of the secrecy capacity is defined as the probability that the secrecy capacity C_s falls below the target secrecy rate R_s, i.e.,

$$P_{out}(R_s) = Pr(C_s < R_s). \tag{A V-17}$$

Secrecy outage probability can be conceptually explained as two cases: (i) $C_s < R_s$ whilst positive secrecy capacity is guaranteed; (ii) $P_{out}(R_s)$ definitely happens when the secrecy capacity is non-positive. (A V-17) can thus be rewritten as follows Ahn *et al.* (2015)

$$\begin{aligned} P_{out}(R_s) &= Pr(C_s<R_s|\gamma_B>\gamma_E)Pr(\gamma_B>\gamma_E)+Pr(\gamma_B<\gamma_E) \\ &= \int_0^{\infty}\int_{\gamma_E}^{\gamma_0} f_{\gamma_B}(\gamma_B)f_{\gamma_E}(\gamma_E)d\gamma_B d\gamma_E + \int_0^{\infty}\int_0^{\gamma_E} f_{\gamma_B}(\gamma_B)f_{\gamma_E}(\gamma_E)d\gamma_B d\gamma_E \\ &= \int_0^{\infty} f_{\gamma_E}(\gamma_E)\left[\int_0^{\gamma_0}-\int_0^{\gamma_E}\right] f_{\gamma_B}(\gamma_B)d\gamma_B d\gamma_E + \int_0^{\infty}\int_0^{\gamma_E} f_{\gamma_B}(\gamma_B)f_{\gamma_E}(\gamma_E)d\gamma_B d\gamma_E \\ &= \int_0^{\infty} F_{\gamma_B}(\gamma_0)f_{\gamma_E}(\gamma_E)d\gamma_E, \end{aligned} \tag{A V-18}$$

where $\gamma_0 = M(1+\gamma_E)-1$, $M = 2^{R_s}$.

Similarly, substituting (A V-8) and (A V-12) into (A V-18) using (A V-15), the closed-form expression for secrecy outage probability can be eventually derived as in (A V-19)

$$P_{out}(R_s) = 1 - \frac{\exp(\frac{1-M}{\Omega_B})}{6\Omega_B^3\Omega_E^4}\left[120M^3(\frac{M}{\Omega_B}+\frac{1}{\Omega_E})^{-7} + 60M^2(\Omega_B - 1 + M)(\frac{M}{\Omega_B}+\frac{1}{\Omega_E})^{-6}\right.$$
$$+ 12M\left(1 - 2\Omega_B + 2\Omega_B^2 - 2M + 2\Omega_B M + M^2\right)(\frac{M}{\Omega_B}+\frac{1}{\Omega_E})^{-5}$$
$$\left.+ \left(-1 + 6\Omega_B^3 + 3\Omega_B - 6\Omega_B^2 + 3M - 6\Omega_B M + 6\Omega_B^2 M - 3M^2 + 3\Omega_B M^2 + M^3\right)(\frac{M}{\Omega_B}+\frac{1}{\Omega_E})^{-4}\right]. \quad \text{(A V-19)}$$

5. Numerical Results and discussions

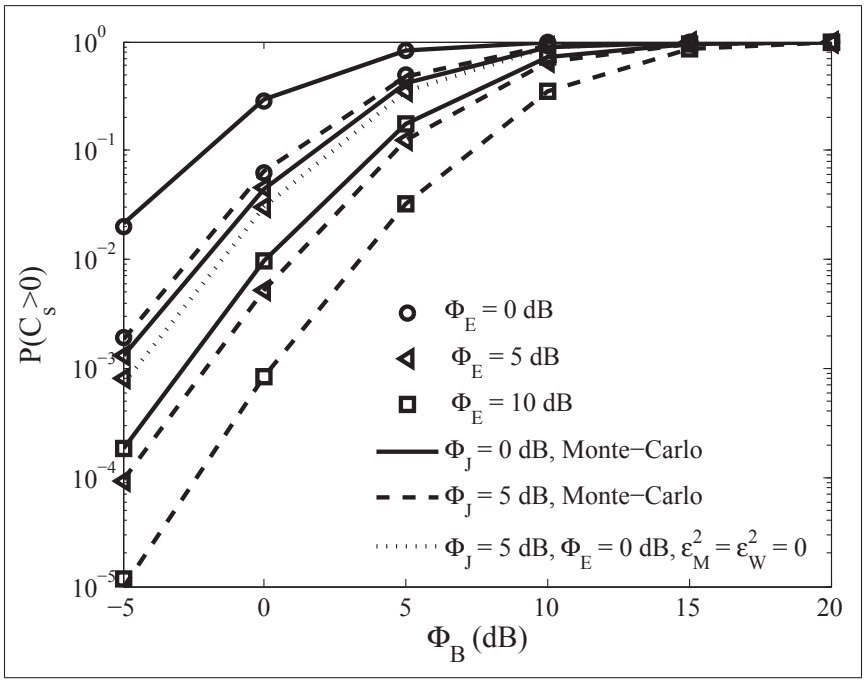


Figure-A V-3 Probability of positive secrecy capacity against Φ_B for selected values of Φ_E for the case of Φ_J = 0 dB and Φ_J = 5 dB whilst $\varepsilon_M^2 = 0.01$, $\varepsilon_W^2 = 0.1$

In this section, we perform the Monte-Carlo simulation to validate the accuracy of the closed-form expressions for probability of positive secrecy capacity and secrecy outage probability. In

the following figures, the curves only using markers are the theoretical results, while the ones in lines are the Monte-Carlo simulation results.

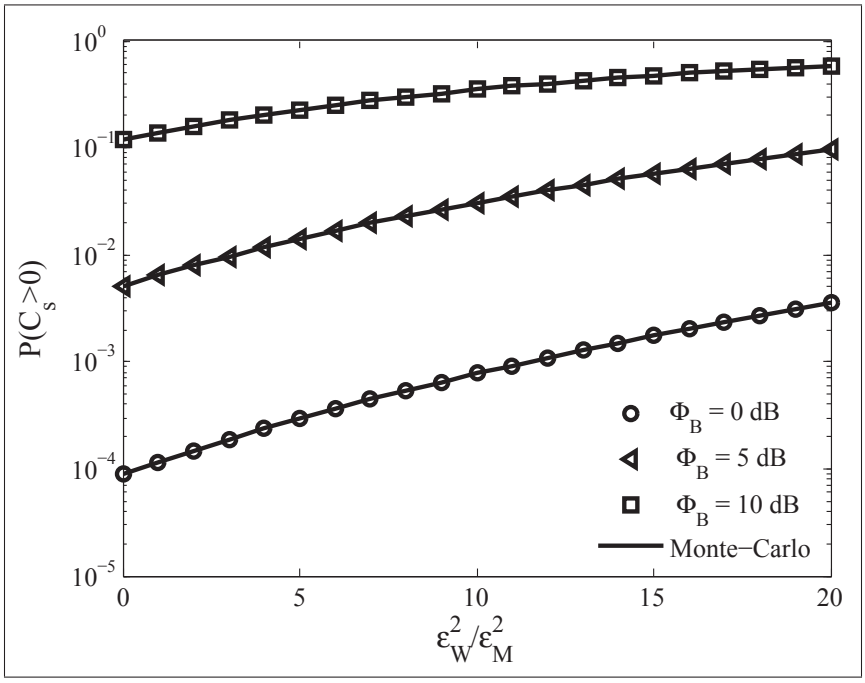


Figure-A V-4 Probability of positive secrecy capacity against $\varepsilon_W^2/\varepsilon_M^2$ for selected values of Φ_B while $\varepsilon_M^2 = 0.01$, Φ_J = 5 dB and Φ_E = 5 dB

Fig. V-3 shows the simulation and analytic results of the probability of positive secrecy capacity against Φ_B for selected values of Φ_E when $\varepsilon_M^2 = 0.01$ and $\varepsilon_W^2 = 0.1$ for the cases: (i) Φ_J = 0 dB, (ii) Φ_J = 5 dB.

One can observe that the numerical results are in perfect match with our analytical results. Notably, we can obtain the conclusions below: (i) $\Pr(C_s > 0)$ increases with Φ_B for a fixed Φ_E. (ii) The higher Φ_E, the lower of probability of positive secrecy capacity. (iii) More importantly, the jamming power Φ_J has a critical role to play in the probability of positive secrecy capacity for fixed γ_E. The larger values of Φ_J, the worse of $\Pr(C_s > 0)$. (iv) Additionally, there exists secrecy loss of imperfect CSI compared with the case of perfect channel estimation (ε_M^2 = 0 and ε_W^2 = 0) at receiver sides.

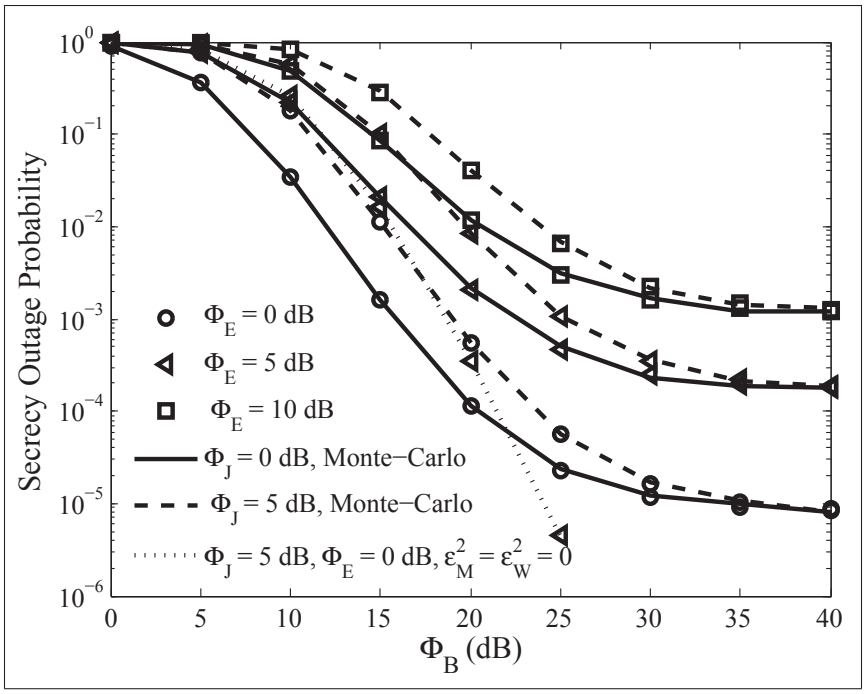


Figure-A V-5 Secrecy outage probability against Φ_B for selected values of Φ_E for the case of Φ_J = 0 dB and Φ_J = 5 dB whilst $\varepsilon_M^2 = 0.01$, $\varepsilon_W^2 = 0.1$ and $R_s = 0.5$ [bits/s/Hz]

Fig. V-4 explores the relationship of probability of positive secrecy capacity against the ratio of ε_W^2 and ε_M^2 whilst $\varepsilon_M^2 = 0.01$, Φ_J = 5 dB and Φ_E = 5 dB for selected values of Φ_B. It is saying that the higher the ratio, the much probable the event that the positive secrecy capacity can be achieved.

Similarly, Fig. V-5 and Fig. V-6 examine the simulation and analysis results of the secrecy outage probability of physical layer security with regard to two cases: (i) fixed ε_M^2 and ε_W^2 whilst varying Φ_B and Φ_E; (ii) changing the ratio of ε_B^2 and ε_W^2 while fixing Φ_J = 5 dB and Φ_E = 5 dB for selected values of Φ_B, namely, 10 dB, 15 dB and 25 dB. Notably, we can easily draw the same conclusion about the accuracy of our derived expression with Monte-Carlo simulation results.

Additionally, as shown in Fig. V-5, the secrecy outage probability degrades with the increase of Φ_B for specific values Φ_E and Φ_J.

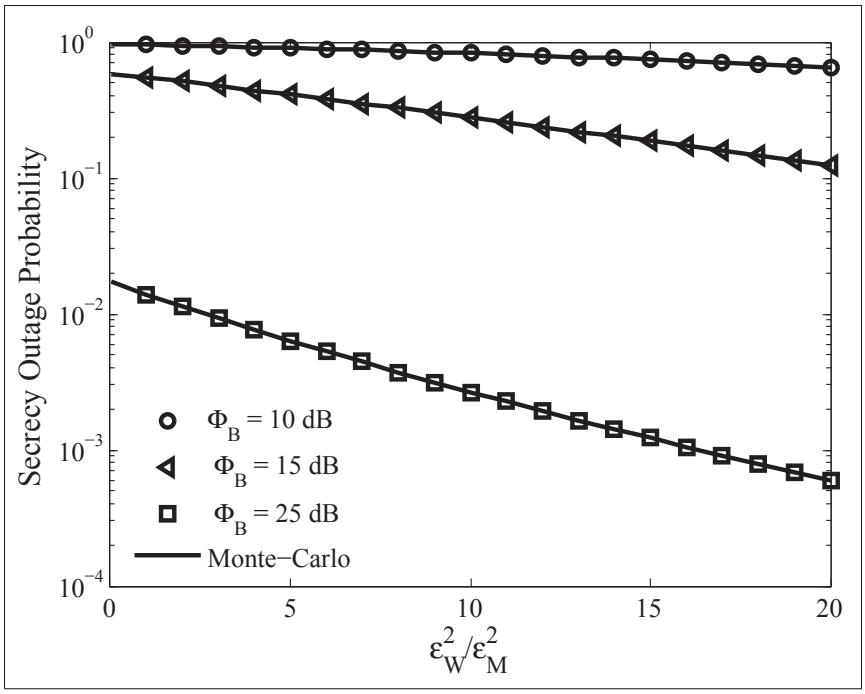


Figure-A V-6 Secrecy outage probability against $\varepsilon_W^2/\varepsilon_M^2$ for selected values of Φ_B while $\varepsilon_M^2 = 0.01$, Φ_J = 5 dB, Φ_E = 5 and $R_s = 0.5$ [bits/s/Hz]

More importantly, there exists an error floor due to the imperfect channel estimation at the receiver sides in comparison with the case, i.e., $\varepsilon_M^2 = 0$ and $\varepsilon_W^2 = 0$. As Φ_B is much larger than Φ_J regarding a fixed Φ_E, Ω_B converges to the same value for different Φ_J with a limited value, which consequently makes their secrecy outage probabilities converge to the error floor.

When it comes to Fig. V-6, the secrecy outage probability witnesses a completely opposite trend compared with that of the probability of positive secrecy capacity, shown in Fig. V-4. Furthermore, the larger of the gap between Φ_B and Φ_E, the less likely the secrecy outage probability.

6. Conclusion

In this paper, we have analyzed secrecy performance of the MIMO wiretap channel with channel estimation errors at the legitimate destination and eavesdropper's receivers whilst in the

presence of an active eavesdropper. The probability of positive secrecy capacity and secrecy outage probability were derived with closed-form expressions through the PDFs and CDFs of the receive SINRs. Finally, the theoretical analysis are confirmed by the Monte-Carlo simulation results by comparing the secrecy performances with different levels of channel estimation errors, received SINRs and jamming signals.

REFERENCES

Wolfram Language & System Documentation Center. Consulted at http://reference.wolfram .com/language/ref/MeijerG.html.

Aalo, V. A., Piboongungon, T. & Iskander, C. D. (2005). Bit-error rate of binary digital modulation schemes in generalized gamma fading channels. *IEEE Commun. Lett.*, 9(2), 139-141.

Abromowitz, M. & Stegun, I. A. (1968). *Handbook of Mathematical Functions: With Formulas, Graphs and Mathematical Tables*. Dover.

Aggarwal, V., Sankar, L., Calderbank, A. & Poor, H. (2009, Jun.). Information secrecy from multiple eavesdroppers in orthogonal relay channels. *IEEE Int. Symp. Inf. Theory*, pp. 2607-2611.

Ahn, K. S., Choi, S.-W. & Ahn, J.-M. (2015). Secrecy Performance of Maximum Ratio Diversity With Channel Estimation Error. *IEEE Signal Process. Lett.*, 22(11), 2167-2171.

Ai , Y., Kong, L. & Cheffena, M. (2019). Secrecy outage analysis of double shadowed Rician channels. *Electron. Lett.*

Al-Hmood, H. & Al-Raweshidy, H. S. (2017). Unified Modeling of Composite $\kappa-\mu$/Gamma, $\eta-\mu$/Gamma, and $\alpha-\mu$/Gamma Fading Channels Using a Mixture Gamma Distribution With Applications to Energy Detection. *IEEE Antennas Wireless Propag. Lett*, 16, 104-108.

Alghorani, Y., Kaddoum, G., Muhaidat, S., Pierre, S. & Al-Dhahir, N. (2016). On the Performance of Multihop-Intervehicular Communications Systems Over n*Rayleigh Fading Channels. *IEEE Wireless Commun. Lett.*, 5(2), 116-119.

Alhennawi, H. R., Ayadi, M. M. H. E., Ismail, M. H. & Mourad, H. A. M. (2016). Closed-Form Exact and Asymptotic Expressions for the Symbol Error Rate and Capacity of the H-Function Fading Channel. *IEEE Trans. Veh. Technol.*, 65(4), 1957-1974.

Allen, T. & Al-Dhahir, N. (2015, Mar.). Performance analysis of a secure STBC with coherent and differential detection. *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 522-527.

Ansari, I. S., Al-Ahmadi, S., Yilmaz, F., Alouini, M. & Yanikomeroglu, H. (2011). A New Formula for the BER of Binary Modulations with Dual-Branch Selection over Generalized-K Composite Fading Channels. *IEEE Trans. Commun.*, 59(10), 2654-2658.

Ansari, I. S., Yilmaz, F. & Alouini, M. S. (2013, Jun.). On the Sum of Squared $\eta - \mu$ Random Variates with Application to the Performance of Wireless Communication Systems. *IEEE 77th VTC Spring*, pp. 1-6.

Atallah, M., Kaddoum, G. & Kong, L. (2015, Oct.). A Survey on Cooperative Jamming Applied to Physical Layer Security. *2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, pp. 1-5. doi: 10.1109/ICUWB.2015.7324413.

Atapattu, S., Tellambura, C. & Jiang, H. (2011). A Mixture Gamma Distribution to Model the SNR of Wireless Channels. *IEEE Trans. Wireless Commun.*, 10(12), 4193-4203.

Ayadi, M. M. H. E., Ismail, M. H. & Alhennawi, H. R. (2016). Unified approach for probability of detection evaluation over generalised fading channels. *IET Commun.*, 10(12), 1532-1541.

Badarneh, O. S. & Almehmadi, F. S. (2016). Performance of Multihop Wireless Networks in $\alpha - \mu$ Fading Channels Perturbed by an Additive Generalized Gaussian Noise. *IEEE Commun. Lett*, 20(5), 986-989.

Badarneh, O. S. & Aloqlah, M. S. (2016). Performance Analysis of Digital Communication Systems Over $\alpha - \eta - \mu$ Fading Channels. *IEEE Trans. Veh. Technol.*, 65(10), 7972-7981.

Badarneh, O. S., da Costa, D. B., Sofotasios, P. C., Muhaidat, S. & Cotton, S. L. (2018). On the Sum of Fisher-Snedecor $\mathscr{F}$ Variates and its Application to Maximal-Ratio Combining. *IEEE Wireless Commun. Lett.*, 1-1.

Badarneh, O. S. (2016). The $\alpha - \mu/\alpha - \mu$ composite multipath-shadowing distribution and its connection with the extended generalized-K distribution. *AEU - International J. Electronics and Commun.*, 70(9), 1211 - 1218.

Bagherikaram, G., Motahari, A. & Khandani, A. (2013). The Secrecy Capacity Region of the Gaussian MIMO Broadcast Channel. *IEEE Trans. Inf. Theory*, 59(5), 2673-2682.

Bai, J., Tao, X., Xu, J. & Cui, Q. (2014). The Secrecy Outage Probability for the *i*th Closest Legitimate User in Stochastic Networks. *IEEE Commun. Lett.*, 18(7), 1230-1233.

Bashar, S., Ding, Z. & Xiao, C. (2012). On Secrecy Rate Analysis of MIMO Wiretap Channels Driven by Finite-Alphabet Input. *IEEE Trans. Commun.*, 60(12), 3816-3825.

Behnad, A., Shahbaz, M. B., Willink, T. J. & Wang, X. (2017). Statistical Analysis and Minimization of Security Vulnerability Region in Amplify-and-Forward Cooperative Systems. *IEEE Trans. Wireless Commun.*, 16(4), 2534-2547.

Bekkali, A., Zou, S., Kadri, A., Crisp, M. & Penty, R. V. (2015). Performance Analysis of Passive UHF RFID Systems Under Cascaded Fading Channels and Interference Effects.

IEEE Trans. Wireless Commun., 14(3), 1421-1433.

Bhargav, N., Cotton, S. L. & Simmons, D. E. (2016). Secrecy Capacity Analysis Over κ-μ Fading Channels: Theory and Applications. *IEEE Trans. Commun.*, 64(7), 3011-3024.

Bloch, M., Barros, J., Rodrigues, M. R. D. & McLaughlin, S. W. (2008). Wireless Information-Theoretic Security. *IEEE Trans. Inf. Theory*, 54(6), 2515-2534.

Bloch, M. & Barros, J. (2011). *Physical-layer security: from information theory to security engineering*. Cambridge University Press.

Bodenschatz, C. D. (1992). *Finding an H-function distribution for the sum of independent H-function variates*. (Ph.D. thesis).

Boulogeorgos, A. A. A., Sofotasios, P. C., Selim, B., Muhaidat, S., Karagiannidis, G. K. & Valkama, M. (2016). Effects of RF Impairments in Communications Over Cascaded Fading Channels. *IEEE Trans. Veh. Technol.*, 65(11), 8878-8894.

Brodtkorb, P., Johannesson, P., Lindgren, G., Rychlik, I., Rydén, J. & Sjö, E. (2000). WAFO - a Matlab Toolbox for the Analysis of Random Waves and Loads. *Proc. 10'th Int. Offshore and Polar Eng. Conf., ISOPE, Seattle, USA*, 3, 343–350.

Chen, G. & Coon, J. P. (2017). Secrecy Outage Analysis in Random Wireless Networks With Antenna Selection and User Ordering. *IEEE Wireless Commun. Lett.*, 6(3), 334-337.

Chen, G., Coon, J. P. & Renzo, M. D. (2017a). Secrecy Outage Analysis for Downlink Transmissions in the Presence of Randomly Located Eavesdroppers. *IEEE Trans. Inf. Forens. Security*, 12(5), 1195-1206.

Chen, X. & Yin, R. (2013). Performance Analysis for Physical Layer Security in Multi-Antenna Downlink Networks with Limited CSI Feedback. *IEEE Wireless Commun. Lett.*, 2(5), 503-506.

Chen, X., Ng, D. W. K., Gerstacker, W. H. & Chen, H. (2017b). A Survey on Multiple-Antenna Techniques for Physical Layer Security. *IEEE Commun. Surveys Tutorials*, 19(2), 1027-1053.

Chergui, H., Benjillali, M. & Saoudi, S. (2016). Performance Analysis of Project-and-Forward Relaying in Mixed MIMO-Pinhole and Rayleigh Dual-Hop Channel. *IEEE Commun. Lett.*, 20(3), 610-613.

Chergui, H., Benjillali, M. & Alouini, M.-S. (2018). Rician K-factor-based analysis of XLOS service probability in 5G outdoor ultra-dense networks,. Consulted at https://arxiv.org/abs/1804.08101.

Cho, S., Chen, G. & Coon, J. P. (2018). Physical Layer Security in Visible Light Communication Systems With Randomly Located Colluding Eavesdroppers. *IEEE Wireless Commun. Lett.*, 7(5), 768-771.

Chong, P. K., Yoo, S. E., Kim, S. H. & Kim, D. (2011). Wind-Blown Foliage and Human-Induced Fading in Ground-Surface Narrowband Communications at 400 MHz. *IEEE Trans. Veh. Technol.*, 60(4), 1326-1336.

Choo, L.-C. & Wong, K.-K. (2009, Nov.). Physical layer security for a 3-receiver broadcast channel. *Int. Conf. Wireless Communications Signal Processing*, pp. 1-5.

Cogliatti, R., de Souza, R. A. A. & Yacoub, M. D. (2012). Practical, Highly Efficient Algorithm for Generating $\kappa-\mu$ and $\eta-\mu$ Variates and a Near-100$\alpha-\mu$ Variates. *IEEE Commun. Lett.*, 16(11), 1768-1771.

Cook Jr, I. D. (1981). *The H-function and probability density functions of certain algebraic combinations of independent random variables with H-function probability distribution*. (Ph.D. thesis).

Csiszar, I. & Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3), 339-348.

da Costa, D. B., Yacoub, M. D. & Filho, J. C. S. S. (2008). Highly accurate closed-form approximations to the sum of α-μ variates and applications. *IEEE Trans. Wireless Commun.*, 7(9), 3301-3306.

da Silva, C. R. N., Leonardo, E. J. & Yacoub, M. D. (2018). Product of Two Envelopes Taken From $\alpha-\mu$, $\kappa-\mu$, and $\eta-\mu$ Distributions. *IEEE Trans. Commun.*, 66(3), 1284-1295.

Debnath, L. & Bhatta, D. (2014). *Integral transforms and their applications*. CRC press.

Deng, Y., Wang, L., Elkashlan, M., Nallanathan, A. & Mallik, R. K. (2016). Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach. *IEEE Trans.Inf. Forens. Security*, 11(6), 1128-1138.

Di Renzo, M. & Debbah, M. (2009, Oct.). Wireless physical-layer security: The challenges ahead. *Int. Conf. Advanced Technologies for Communications*, pp. 313-316.

Dias, U. S. & Yacoub, M. D. (2009, Nov.). On the $\alpha-\mu$ Autocorrelation and Power Spectrum Functions: Field Trials and Validation. *IEEE GLOBECOM*, pp. 1-6.

Duruturk, M. (2010). Study of Physical Layer Security in Wireless Communications. *Dissertations & Student Research in Computer Electronics & Engineering*, 4.

Erceg, V., Fortune, S. J., Ling, J., Rustako, A. J. & Valenzuela, R. A. (1997). Comparisons of a computer-based propagation prediction tool with experimental data collected in urban

microcellular environments. *IEEE J. Sel. Areas Commun.*, 15(4), 677-684.

Ericsson. (2018). 10 hot consumer trends 2019. Consulted at https://www.ericsson.com/en/trends-and-insights/consumerlab/consumer-insights/reports/10-hot-consumer-trends-2019.

Goel, S. & Negi, R. (2005, Oct.). Secret communication in presence of colluding eavesdroppers. *Proc. Military Commun. Conf.*, pp. 1501-1506.

Gopala, P. K., Lai, L. & Gamal, H. E. (2008). On the Secrecy Capacity of Fading Channels. *IEEE Trans. Inf. Theory*, 54(10), 4687-4698. doi: 10.1109/TIT.2008.928990.

Gradshteyn, I. S. & Ryzhik, I. M. (2014). *Table of integrals, series, and products*. Academic press.

Gupta, S. (1969). Integrals involving products of G-functions. *Proc. Nat. Acad. Sci., India*, 539-542.

Haenggi, M. (2008a, Jul.). The secrecy graph and some of its properties. *IEEE ISIT*, pp. 539-543.

Haenggi, M. (2008b). A Geometric Interpretation of Fading in Wireless Networks: Theory and Applications. *IEEE Trans. Inf. Theory*, 54(12), 5500-5510.

Haenggi, M. (2012). *Stochastic geometry for wireless networks*. Cambridge University Press.

Hajri, N., Youssef, N. & Patzold, M. (2016). On the Statistical Properties of Phase Crossings and Random FM Noise in Double Rayleigh Fading Channels. *IEEE Trans. Veh. Technol.*, 65(4), 1859-1867.

Hajri, N., Youssef, N., Kawabata, T., Patzold, M. & Dahech, W. (2018). Statistical Properties of Double Hoyt Fading With Applications to the Performance Analysis of Wireless Communication Systems. *IEEE Access*, 6, 19597-19609.

Hong, Y.-W. P., Lan, P.-C. & Kuo, C.-C. J. (2013). *Signal processing approaches to secure physical layer communications in multi-antenna wireless systems*. Springer Science & Business Media.

Hu, J., Yang, W., Yang, N., Zhou, X. & Cai, Y. (2016). On-Off-Based Secure Transmission Design With Outdated Channel State Information. *IEEE Trans. Veh. Technol.*, 65(8), 6075-6088.

Ilhan, H. (2012). Performance Analysis of Two-Way AF Relaying Systems Over Cascaded Nakagami- *m* Fading Channels. *IEEE Signal Process. Lett.*, 19(6), 332-335.

Iwata, S., Ohtsuki, T. & Kam, P. Y. (2017, May). Secure outage probability over $\kappa - \mu$ fading channels. *2017 IEEE Int. Conf. Commun. (ICC)*, pp. 1-6.

Jameel, F., Wyne, S. & Krikidis, I. (2017). Secrecy Outage for Wireless Sensor Networks. *IEEE Commun. Lett.*, 21(7), 1565-1568.

Jameel, F., Wyne, S., Kaddoum, G. & Duong, T. Q. (2018). A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Commun. Surveys Tutorials*, 1-1.

Jeong, Y., Chong, J. W., Shin, H. & Win, M. Z. (2013). Intervehicle Communication: Cox-Fox Modeling. *IEEE J. Sel. Areas Commun.*, 31(9), 418-433.

Jeong, Y., Quek, T. Q. S., Kwak, J. S. & Shin, H. (2014). Multicasting in Stochastic MIMO Networks. *IEEE Trans. Wireless Commun.*, 13(4), 1-13.

Jorswieck, E., Tomasin, S. & Sezgin, A. (2015). Broadcasting Into the Uncertainty: Authentication and Confidentiality by Physical-Layer Processing. *Proc. of the IEEE*, 103(10), 1702-1724.

Kamel, M., Hamouda, W. & Youssef, A. (2017). Physical Layer Security in Ultra-Dense Networks. *IEEE Wireless Commun. Lett.*, 6(5), 690-693.

Kapetanovic, D., Zheng, G. & Rusek, F. (2015). Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Commun. Mag.*, 53(6), 21-27.

Karadimas, P., Vagenas, E. D. & Kotsopoulos, S. A. (2010). On the Scatterers' Mobility and Second Order Statistics of Narrowband Fixed Outdoor Wireless Channels. *IEEE Trans. Wireless Commun.*, 9(7), 2119-2124.

Karagiannidis, G. K., Sagias, N. C. & Mathiopoulos, P. T. (2007). N*Nakagami: A Novel Stochastic Model for Cascaded Fading Channels. *IEEE Trans. Commun.*, 55(8), 1453-1458.

Khisti, A. & Wornell, G. W. (2010a). Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel. *IEEE Trans. Inf. Theory*, 56(7), 3088-3104.

Khisti, A. & Wornell, G. W. (2010b). Secure Transmission With Multiple Antennas — Part II: The MIMOME Wiretap Channel. *IEEE Trans. Inf. Theory*, 56(11), 5515-5532.

Khisti, A., Wornell, G., Wiesel, A. & Eldar, Y. (2007, Jun.). On the Gaussian MIMO Wiretap Channel. *IEEE Int. Symp. Inf. Theory*, pp. 2471-2475.

Khisti, A., Tchamkerten, A. & Wornell, G. W. (2008). Secure Broadcasting Over Fading Channels. *IEEE Trans. Inf. Theory*, 54(6), 2453-2469.

Khisti, A. & Wornell, G. (2007). The MIMOME channel. *arXiv preprint arXiv:0710.1325*.

Kong, L. & Kaddoum, G. (2018). On Physical Layer Security Over the Fisher-Snedecor $\mathscr{F}$ Wiretap Fading Channels. *IEEE Access*, 6(1), 39466-39472.

Kong, L. & Kaddoum, G. (2019). Secrecy Characteristics with Assistance of Mixture Gamma Distribution. *IEEE Wireless Commun. Lett.*

Kong, L., He, J., Kaddoum, G., Vuppala, S. & Wang, L. (2016a, Sept.). Secrecy Analysis of a MIMO Full-Duplex Active Eavesdropper with Channel Estimation Errors. *Proc. 2016 IEEE VTC-Fall*, pp. 1-5.

Kong, L., Tran, H. & Kaddoum, G. (2016b). Performance analysis of physical layer security over $\alpha - \mu$ fading channel. *Electron. Lett.*, 52(1), 45-47.

Kong, L., Kaddoum, G. & da Costa, D. B. (2018a). Cascaded $\alpha - \mu$ Fading Channels: Reliability and Security Analysis. *IEEE Access*, 6, 41978-41992.

Kong, L., Kaddoum, G., da Costa, D. B. & Bou-Harb, E. (2018b, Jun.). On Secrecy Bounds of MIMO Wiretap Channels with ZF detectors. *2018 14th Intl Wireless Commun. Mobile Computing Conf.(IWCMC)*, pp. 724-729.

Kong, L., Kaddoum, G. & Rezki, Z. (2018c). Highly Accurate and Asymptotic Analysis on the SOP Over SIMO $\alpha - \mu$ Fading Channels. *IEEE Commun. Lett.*, 22(10), 2088-2091. doi: 10.1109/LCOMM.2018.2861877.

Kong, L., Kaddoum, G. & Vuppala, S. (2018d, May). On Secrecy Analysis for D2D Networks over $\alpha - \mu$ Fading Channels with Randomly Distributed Eavesdroppers. *2018 IEEE Intl Conf. Commun. Workshops (ICC Workshops)*, pp. 1-6.

Kong, L., Vuppala, S. & Kaddoum, G. (2018e). Secrecy Analysis of Random MIMO Wireless Networks Over α-μ Fading Channels. *IEEE Trans. Veh. Technol.*, 67(12), 11654-11666.

Kong, N. & Milstein, L. B. (1999). Average SNR of a generalized diversity selection combining scheme. *IEEE Commun. Lett.*, 3(3), 57-59.

Kumar, S., Chandrasekaran, G. & Kalyani, S. (2015). Analysis of Outage Probability and Capacity for κ - μ/η - μ Faded Channel. *IEEE Commun. Lett.*, 19(2), 211-214.

Kwon, T., Wong, V. & Schober, R. (2012, Dec.). Secure MISO cognitive radio system with perfect and imperfect CSI. *IEEE Global Commun. Conf. (GLOBECOM)*, pp. 1236-1241.

Lai, L. & Gamal, H. E. (2008). The Relay Eavesdropper Channel: Cooperation for Secrecy. *IEEE Trans. Inf. Theory*, 54(9), 4005-4019.

Lai, L., El Gamal, H. & Poor, H. (2008). The Wiretap Channel With Feedback: Encryption Over the Channel. *IEEE Trans. Inf. Theory*, 54(11), 5059-5067.

Laourine, A., Alouini, M. S., Affes, S. & Stephenne, A. (2009). On the performance analysis of composite multipath/shadowing channels using the *G*-distribution. *IEEE Trans. Commun.*, 57(4), 1162-1170.

Lee, E.-K., Gerla, M. & Oh, S. (2012). Physical layer security in wireless smart grid. *IEEE Commun. Mag.*, 50(8), 46-52.

Lei, H., Gao, C., Guo, Y. & Pan, G. (2015). On Physical Layer Security Over Generalized Gamma Fading Channels. *IEEE Commun. Lett.*, 19(7), 1257-1260.

Lei, H., Ansari, I. S., Gao, C., Guo, Y., Pan, G. & Qaraqe, K. A. (2016a). Physical-layer security over generalised-K fading channels. *IET Commun.*, 10(16), 2233-2237.

Lei, H., Gao, C., Ansari, I. S., Guo, Y., Pan, G. & Qaraqe, K. A. (2016b). On Physical-Layer Security Over SIMO Generalized-K Fading Channels. *IEEE Trans. Veh. Technol.*, 65(9), 7780-7785.

Lei, H., Zhang, H., Ansari, I. S., Gao, C., Guo, Y., Pan, G. & Qaraqe, K. A. (2016c). Performance Analysis of Physical Layer Security Over Generalized-K Fading Channels Using a Mixture Gamma Distribution. *IEEE Commun. Lett.*, 20(2), 408-411.

Lei, H., Ansari, I. S., Pan, G., Alomair, B. & Alouini, M. S. (2017a). Secrecy Capacity Analysis Over $\alpha - \mu$ Fading Channels. *IEEE Commun. Lett.*, 21(6), 1445-1448.

Lei, H., Dai, Z., Ansari, I. S., Park, K. H., Pan, G. & Alouini, M. S. (2017b). On Secrecy Performance of Mixed RF-FSO Systems. *IEEE Photon. J.*, 9(4), 1-14.

Lei, H., Luo, H., Park, K. H., Ren, Z., Pan, G. & Alouini, M. S. (2018a). Secrecy Outage Analysis of Mixed RF-FSO Systems With Channel Imperfection. *IEEE Photon. J.*, 10(3), 1-13.

Lei, H., Zhang, J., Park, K. H., Xu, P., Zhang, Z., Pan, G. & Alouini, M. S. (2018b). Secrecy Outage of Max-Min TAS Scheme in MIMO-NOMA Systems. *IEEE Trans. Veh. Technol.*, 1-1.

Leonardo, E. J. & Yacoub, M. D. (2015a). The Product of Two $\alpha - \mu$ Variates and the Composite $\alpha - \mu$ Multipath-Shadowing Model. *IEEE Trans. Veh. Technol.*, 64(6), 2720-2725.

Leonardo, E. J. & Yacoub, M. D. (2015b). Product of $\alpha - \mu$ Variates. *IEEE Wireless Commun. Lett.*, 4(6), 637-640.

Leonardo, E. J., Yacoub, M. D. & de Souza, R. A. A. (2016). Ratio of Products of $\alpha - \mu$ Variates. *IEEE Commun. Lett.*, 20(5), 1022-1025.

Leung-Yan-Cheong, S. & Hellman, M. (1978). The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4), 451-456.

Leung-Yan-Cheong, S. K. (1976). *Multi-User and Wiretap Channels Including Feedback.*

Li, N., Tao, X. & Xu, J. (2014). Ergodic Secrecy Sum-Rate for Downlink Multiuser MIMO Systems With Limited CSI Feedback. *IEEE Commun. Lett.*, 18(6), 969-972.

Li, N., Tao, X., Wu, H., Xu, J. & Cui, Q. (2016). Large-System Analysis of Artificial-Noise-Assisted Communication in the Multiuser Downlink: Ergodic Secrecy Sum Rate and Optimal Power Allocation. *IEEE Trans. Veh. Technol.*, 65(9), 7036-7050.

Liang, Y., Poor, H. & Shamai, S. (2008). Secure Communication Over Fading Channels. *IEEE Trans. Inf. Theory*, 54(6), 2470-2492.

Lin, M., Lin, Z., Zhu, W. & Wang, J. (2018). Joint Beamforming for Secure Communication in Cognitive Satellite Terrestrial Networks. *IEEE J. Sel. Areas Commun.*, 36(5), 1017-1029.

Liu, R. & Poor, H. (2008, Jul.). Multi-antenna Gaussian broadcast channels with confidential messages. *IEEE Int. Symp. Inf. Theory*, pp. 2202-2206.

Liu, R., Maric, I., Spasojevic', P. & Yates, R. (2008a). Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions. *IEEE Trans. Inf. Theory*, 54(6), 2493-2507.

Liu, T. & Shamai, S. (2009). A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel. *IEEE Trans. Inf. Theory*, 55(6), 2547-2553.

Liu, T., Prabhakaran, V. & Vishwanath, S. (2008b, Jul.). The secrecy capacity of a class of parallel Gaussian compound wiretap channels. *IEEE Int. Symp. Inf. Theory*, pp. 116-120.

Liu, W., Vuppala, S., Abreu, G. & Ratnarajah, T. (2014, Sep.). Secrecy outage in correlated Nakagami-m fading channels. *2014 IEEE 25th Annual International Symp. Personal, Indoor, and Mobile Radio Communication (PIMRC)*, pp. 145-149.

Liu, W., Ding, Z., Ratnarajah, T. & Xue, J. (2016). On Ergodic Secrecy Capacity of Random Wireless Networks With Protected Zones. *IEEE Trans. Veh. Technol.*, 65(8), 6146-6158.

Liu, X. (2013a). Probability of Strictly Positive Secrecy Capacity of the Rician-Rician Fading Channel. *IEEE Wireless Commun. Lett.*, 2(1), 50-53.

Liu, X. (2013b, Dec.). Probability of strictly positive secrecy capacity of the Weibull fading channel. *2013 IEEE GLOBECOM*, pp. 659-664.

Liu, Y., Qin, Z., Elkashlan, M., Gao, Y. & Hanzo, L. (2017). Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks. *IEEE Trans. Wireless Commun.*, 16(3), 1656-1672.

Mathai, A. M. (1972). Products and ratios of generalized gamma variates. *Scandinavian Actuarial Journal*, 1972(2), 193-198.

Mathai, A. M. & Saxena, R. K. (1978). *The H-function with applications in statistics and other disciplines*. Wiley.

Mathai, A. M., Saxena, R. K. & Haubold, H. J. (2009a). *The H-function: theory and applications*. Springer Science & Business Media.

Mathai, A. M., Saxena, R. K. & Haubold, H. J. (2009b). *The H-function: theory and applications*. Springer Science & Business Media.

Mathur, A., Ai, Y., Bhatnagar, M. R., Cheffena, M. & Ohtsuki, T. (2018). On Physical Layer Security of α-η-κ-μ Fading Channels. *IEEE Commun. Lett.*, 22(10), 2168-2171.

Michalopoulos, D. S., Suraweera, H. A., Karagiannidis, G. K. & Schober, R. (2012). Amplify-and-Forward Relay Selection with Outdated Channel Estimates. *IEEE Trans. Commun.*, 60(5), 1278-1290.

Michalopoulou, A., Zervos, T., Peppas, K., Lazarakis, F., Alexandridis, A. A., Dangakis, K. & Kaklamani, D. I. (2011, Apr.). On-body diversity channels at 2.45 GHz: Measurements and statistical analysis. *Proc. 5th Eur. Conf. Antennas Propag. (EUCAP)*, pp. 2982-2986.

Michalopoulou, A., Alexandridis, A. A., Peppas, K., Zervos, T., Lazarakis, F., Dangakis, K. & Kaklamani, D. I. (2012). Statistical Analysis for On-Body Spatial Diversity Communications at 2.45 GHz. *IEEE Trans. Antennas Propag.*, 60(8), 4014-4019.

Mittal, P. & Gupta, K. (1972). An integral involving generalized function of two variables. *Proceedings of the Indian Academy of Sciences-Section A*, 75(3), 117–123.

Moosavi, H. & Bui, F. M. (2016). Delay-Aware Optimization of Physical Layer Security in Multi-Hop Wireless Body Area Networks. *IEEE Trans. Inf. Forens. Security*, 11(9), 1928-1939.

Moualeu, J. M. & Hamouda, W. (2017). On the Secrecy Performance Analysis of SIMO Systems Over κ-μ Fading Channels. *IEEE Commun. Lett.*, 21(11), 2544-2547.

Mukherjee, A. (2015). Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proc. IEEE*, 103(10), 1747-1761.

Mukherjee, A. & Swindlehurst, A. (2011, Nov.). A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures. *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, pp. 265-269.

Negi, R. & Goel, S. (2005, Sep.). Secret communication using artificial noise. *IEEE 62nd Vehicular Technology Conference*, 3, 1906-1910.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations. *IEEE Communications Surveys Tutorials*, 1-1.

Oggier, F. & Hassibi, B. (2011). The Secrecy Capacity of the MIMO Wiretap Channel. *IEEE Trans. Inf. Theory*, 57(8), 4961-4972.

Oggier, F. & Hassibi, B. (2015). A Perspective on the MIMO Wiretap Channel. *Proc. IEEE*, 103(10), 1874-1882.

Oohama, Y. (2001, Sep.). Coding for relay channels with confidential messages. *Inf. Theory Workshop*, pp. 87-89.

Oohama, Y. (2007, Jun.). Capacity Theorems for Relay Channels with Confidential Messages. *IEEE Int. Symp. Inf. Theory*, pp. 926-930.

Pan, G., Tang, C., Zhang, X., Li, T., Weng, Y. & Chen, Y. (2016). Physical-Layer Security Over Non-Small-Scale Fading Channels. *IEEE Trans. Veh. Technol.*, 65(3), 1326-1339.

Pan, G., Ye, J. & Ding, Z. (2017). Secure Hybrid VLC-RF Systems With Light Energy Harvesting. *IEEE Trans. Commun.*, 65(10), 4348-4359.

Papazafeiropoulos, A. K. & Kotsopoulos, S. A. (2010). Generalized Phase-Crossing Rate and Random FM Noise for $\alpha - \mu$ Fading Channels. *IEEE Trans. Veh. Technol.*, 59(1), 494-499.

Parada, P. & Blahut, R. (2005, Sep.). Secrecy capacity of SIMO and slow fading channels. *IEEE Int. Symp. Inf. Theory*, pp. 2152-2155.

Peppas, K., Lazarakis, F., Alexandridis, A. & Dangakis, K. (2010). Cascaded generalised-K fading channel. *IET Commun.*, 4(1), 116-124.

Peppas, K. P. (2012). A New Formula for the Average Bit Error Probability of Dual-Hop Amplify-and-Forward Relaying Systems over Generalized Shadowed Fading Channels. *IEEE Wireless Commun. Lett.*, 1(2), 85-88.

Peppas, K. P., Lazarakis, F., Alexandridis, A. & Dangakis, K. (2012). Simple, accurate formula for the average bit error probability of multiple-input multiple-output free-space optical

links over negative exponential turbulence channels. *Optics lett.*, 37(15), 3243–3245.

Pinto, P. C., Barros, J. & Win, M. Z. (2008, Nov.). Physical-layer security in stochastic wireless networks. *2008 11th IEEE Singapore International Conference on Communication Systems*, pp. 974-979.

Pinto, P. C., Barros, J. & Win, M. Z. (2012a). Secure Communication in Stochastic Wireless Networks — Part I: Connectivity. *IEEE Trans. Inf. Forens. Security*, 7(1), 125-138.

Pinto, P. C., Barros, J. & Win, M. Z. (2012b). Secure Communication in Stochastic Wireless Networks — Part II: Maximum Rate and Collusion. *IEEE Trans. Inf. Forens. Security*, 7(1), 139-147.

Poor, H. V. & Schaefer, R. F. (2017). Wireless physical layer security. *Proceedings of the National Academy of Sciences*, 114(1), 19–26. doi: 10.1073/pnas.1618130114.

Prudnikov, A. P., Brychkov, Y. A. & Marichev, O. I. (1990). *Integrals and Series: More special functions*. Gordon and Breach Science Publishers.

Rahama, Y. A., Ismail, M. H. & Hassan, M. S. (2016). Capacity of Fox's *H*-function fading channel with adaptive transmission. *Electron. Lett.*, 52(11), 976-978.

Rahama, Y. A., Ismail, M. H. & Hassan, M. (2018). On the Sum of Independent Fox's *H*-function Variates with Applications. *IEEE Trans. Veh. Technol.*, 67(8), 6752-6760.

Reig, J. & Rubio, L. (2013). Estimation of the Composite Fast Fading and Shadowing Distribution Using the Log-Moments in Wireless Communications. *IEEE Trans. Wireless Commun.*, 12(8), 3672-3681.

Romero-Jerez, J. M. & Lopez-Martinez, F. J. (2017). A New Framework for the Performance Analysis of Wireless Communications Under Hoyt (Nakagami-*q*) Fading. *IEEE Trans. Inf. Theory*, 63(3), 1693-1702.

Saad, W., Zhou, X., Debbah, M. & Poor, H. (2015). Wireless physical layer security: Part 1 [Guest Editorial]. *IEEE Commun. Mag.*, 53(6), 15-15.

Sagias, N. C. & Tombras, G. S. (2007). On the cascaded Weibull fading channel model. *Journal of the Franklin Institute*, 344(1), 1-11.

Sarkar, M. Z. I., Ratnarajah, T. & Sellathurai, M. (2009, Nov.). Secrecy capacity of Nakagami-*m* fading wireless channels in the presence of multiple eavesdroppers. *2009 Conference Record of the Forty-Third Asilomar Conf. Signals, Systems and Computers*, pp. 829-833.

Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons.

Shafiee, S. & Ulukus, S. (2007, Jun.). Achievable Rates in Gaussian MISO Channels with Secrecy Constraints. *IEEE Int. Symp. Inf. Theory*, pp. 2466-2470.

Shafiee, S., Liu, N. & Ulukus, S. (2009). Towards the Secrecy Capacity of the Gaussian MIMO Wire-Tap Channel: The 2-2-1 Channel. *IEEE Trans. Inf. Theory*, 55(9), 4033-4039.

Shannon, C. (1949). Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.*, 28(4), 656-715.

Shiu, Y. S., Chang, S. Y., Wu, H. C., Huang, S. C. H. & Chen, H. H. (2011). Physical layer security in wireless networks: a tutorial. *IEEE Wireless Commun.*, 18(2), 66-74.

Sofotasios, P. C., Mohjazi, L., Muhaidat, S., Al-Qutayri, M. & Karagiannidis, G. K. (2016). Energy Detection of Unknown Signals Over Cascaded Fading Channels. *IEEE Antennas Wireless Propag. Lett.*, 15, 135-138.

Song, Y., Shin, H. & Kim, W. (2008). Asymptotic SEP for M-PSK Signals over $\alpha - \mu$ Fading Channels. *IEEE Commun. Lett.*, 12(9), 675-677.

Stacy, E. W. (1962). A Generalization of the Gamma Distribution. *The Annals of Mathematical Statistics*, 33(3), 1187–1192. Consulted at http://www.jstor.org/stable/2237889.

Talha, B. & Patzold, M. (2011). Channel Models for Mobile-to-Mobile Cooperative Communication Systems: A State of the Art Review. *IEEE Veh. Technol. Mag.*, 6(2), 33-43.

Tang, X., Liu, R., Spasojevic, P. & Poor, H. (2007, Sep.). Multiple Access Channels with Generalized Feedback and Confidential Messages. *IEEE Inf. Theory Workshop*, pp. 608-613.

Tekin, E. & Yener, A. (2007, Jun.). Achievable Rates for Two-Way Wire-Tap Channels. *IEEE Int. Symp. Inf. Theory*, pp. 941-945.

Telatar, I. E. et al. (1999). Capacity of multi-antenna Gaussian channels. *European transactions on telecommunications*, 10(6), 585–595.

Thai, C. D. T., Lee, J. & Quek, T. Q. S. (2016). Physical-Layer Secret Key Generation With Colluding Untrusted Relays. *IEEE Trans. Wireless Commun.*, 15(2), 1517-1530.

Tolossa, Y. J., Vuppala, S. & Abreu, G. (2017). Secrecy-Rate Analysis in Multitier Heterogeneous Networks Under Generalized Fading Model. *IEEE Internet Things J.*, 4(1), 101-110.

Tolossa, Y. J., Vuppala, S., Kaddoum, G. & Abreu, G. (2018). On the Uplink Secrecy Capacity Analysis in D2D-Enabled Cellular Network. *IEEE Systems Journal*, 12(3), 2297-2307.

Tran, D., Tran, H., Ha, D. & Kaddoum, G. (2019). Secure Transmit Antenna Selection Protocol for MIMO NOMA Networks Over Nakagami-m Channels. *IEEE Systems Journal*, 1-12.

Tran, H., Duong, T. Q. & Zepernick, H. (2011, Nov.). On the performance of spectrum sharing systems over $\alpha - \mu$ fading channel for non-identical μ parameter. *2011 8th International Symposium on Wireless Communication Systems*, pp. 477-481.

Trigui, I., Laourine, A., Affes, S. & Stephenne, A. (2009, Nov.). On the Performance of Cascaded Generalized K Fading Channels. *IEEE Global Telecommunications Conference*, pp. 1-5.

Vuppala, S. & Abreu, G. (2016). Asymptotic Secrecy Analysis of Random Networks With Colluding Eavesdroppers. *IEEE Systems J.*, PP(99), 1-10.

Vuppala, S., Biswas, S., Ratnarajah, T. & Sellathurai, M. On the security region of best source indices in random wireless networks. *Proc. 2016 IEEE ICC*, pp. 1-6.

Vuppala, S., Biswas, S. & Ratnarajah, T. (2017). Secrecy Outage Analysis of *k*th Best Link in Random Wireless Networks. *IEEE Trans. Commun.*, 65(10), 4478-4491.

Vuppala, S., Tolossa, Y. J., Kaddoum, G. & Abreu, G. (2018). On the Physical Layer Security Analysis of Hybrid Millimeter Wave Networks. *IEEE Trans. Commun.*, 66(3), 1139-1152.

Wang, C. & Wang, H. M. (2016). Physical Layer Security in Millimeter Wave Cellular Networks. *IEEE Trans. Wireless Commun.*, 15(8), 5569-5585.

Wang, C., Wang, H., Ng, D. W. K., Xia, X. & Liu, C. (2015a). Joint Beamforming and Power Allocation for Secrecy in Peer-to-Peer Relay Networks. *IEEE Trans. Wireless Commun.*, 14(6), 3280-3293.

Wang, C. & Wang, H.-M. (2014). On the Secrecy Throughput Maximization for MISO Cognitive Radio Network in Slow Fading Channels. *IEEE Trans. Inf. Forens. Security*, 9(11), 1814-1827.

Wang, G., Liu, Q., He, R., Gao, F. & Tellambura, C. (2015b). Acquisition of channel state information in heterogeneous cloud radio access networks: challenges and research directions. *IEEE Wireless Commun.*, 22(3), 100-107.

Wang, H., Zhou, X. & Reed, M. C. (2013). Physical Layer Security in Cellular Networks: A Stochastic Geometry Approach. *IEEE Trans. Wireless Commun.*, 12(6), 2776-2787.

Wang, L., Liu, J., Chen, M., Gui, G. & Sari, H. (2018). Optimization-Based Access Assignment Scheme for Physical-Layer Security in D2D Communications Underlaying a Cellular Network. *IEEE Trans. Veh. Technol.*, 67(7), 5766-5777.

Wu, L., Yang, L., Chen, J. & Alouini, M. S. (2018a). Physical Layer Security for Cooperative Relaying Over Generalized-K Fading Channels. *IEEE Wireless Commun. Lett.*, PP(99), 1-1.

Wu, Q., Matolak, D. W. & Sen, I. (2010). 5-GHz-Band Vehicle-to-Vehicle Channels: Models for Multiple Values of Channel Bandwidth. *IEEE Trans. Veh. Technol.*, 59(5), 2620-2625.

Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K. & Gao, X. (2018b). A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE J. Sel. Areas Commun.*, 36(4), 679-695.

Wyner, A. D. (1975). The wire-tap channel. *The Bell System Technical Journal*, 54(8), 1355-1387.

Xiao, L., Wan, X., Lu, X., Zhang, Y. & Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? *IEEE Signal Processing Mag.*, 35(5), 41-49.

Xiao, L., Greenstein, L., Mandayam, N. & Trappe, W. (2007, Jun.). Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication. *IEEE Int. Conf. Commun.*, pp. 4646-4651.

Yacoub, M. D. (2007a). The $\alpha - \mu$: Distribution: A Physical Fading Model for the Stacy Distribution. *IEEE Trans. Veh. Technol.*, 56(1), 27-34.

Yacoub, M. D. (2007b). The κ-μ distribution and the $\eta - \mu$ distribution. *IEEE Antennas Propag. Mag.*, 49(1), 68-81.

Yan, S., Yang, N., Malaney, R. & Yuan, J. (2014). Transmit Antenna Selection with Alamouti Coding and Power Allocation in MIMO Wiretap Channels. *IEEE Trans. Wireless Commun.*, 13(3), 1656-1667.

Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J. & Di Renzo, M. (2015). Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.*, 53(4), 20-27.

Yao, J., Zhou, X., Liu, Y. & Feng, S. (2018). Secure Transmission in Linear Multihop Relaying Networks. *IEEE Trans. Wireless Commun.*, 17(2), 822-834.

Yilmaz, F. & Alouini, M. S. (2009, Nov.). Product of the Powers of Generalized Nakagami-m Variates and Performance of Cascaded Fading Channels. *IEEE Global Telecommun. Conf.*, pp. 1-8.

Yilmaz, F. & Alouini, M. S. (2012). A Novel Unified Expression for the Capacity and Bit Error Probability of Wireless Communication Systems over Generalized Fading Channels. *IEEE Trans. Commun.*, 60(7), 1862-1876.

Yoo, S. K., Cotton, S. L., Sofotasios, P. C., Matthaiou, M., Valkama, M. & Karagiannidis, G. K. (2017). The Fisher-Snedecor $\mathcal{F}$ Distribution: A Simple and Accurate Composite Fading Model. *IEEE Commun. Lett.*, 21(7), 1661-1664.

Zhang, H., Xing, H., Cheng, J., Nallanathan, A. & Leung, V. C. M. (2016a). Secure Resource Allocation for OFDMA Two-Way Relay Wireless Sensor Networks Without and With Cooperative Jamming. *IEEE Trans. Ind. Informat.*, 12(5), 1714-1725.

Zhang, J., Dai, L., Wang, Z., Ng, D. W. K. & Gerstacker, W. H. (2015a, Dec.). Effective Rate Analysis of MISO Systems over α-μ Fading Channels. *IEEE GLOBECOM*, pp. 1-6.

Zhang, M. & Liu, Y. (2016). Energy Harvesting for Physical-Layer Security in OFDMA Networks. *IEEE Trans. Inf. Forens. Security*, 11(1), 154-162.

Zhang, N., Cheng, N., Lu, N., Zhang, X., Mark, J. & Shen, X. (2015b). Partner Selection and Incentive Mechanism for Physical Layer Security. *IEEE Trans. Wireless Commun.*, 14(8), 4265-4276.

Zhang, X., Zhou, X. & McKay, M. R. (2013). Enhancing Secrecy With Multi-Antenna Transmission in Wireless Ad Hoc Networks. *IEEE Trans. Inf. Forens. Security*, 8(11), 1802-1814.

Zhang, Y., Shen, Y., Wang, H., Yong, J. & Jiang, X. (2016b). On Secure Wireless Communications for IoT Under Eavesdropper Collusion. *IEEE Trans. Autom. Sci. Eng.*, 13(3), 1281-1293.

Zhao, R., Lin, H., He, Y. C., Chen, D. H., Huang, Y. & Yang, L. (2018). Secrecy Performance of Transmit Antenna Selection for MIMO Relay Systems With Outdated CSI. *IEEE Trans. Commun.*, 66(2), 546-559.

Zheng, G., Arapoglou, P. & Ottersten, B. (2012). Physical Layer Security in Multibeam Satellite Systems. *IEEE Trans. Wireless Commun.*, 11(2), 852-863.

Zheng, T. X., Wang, H. M. & Yin, Q. (2014). On Transmission Secrecy Outage of a Multi-Antenna System With Randomly Located Eavesdroppers. *IEEE Commun. Lett.*, 18(8), 1299-1302.

Zheng, Z. (2015). Statistical Analysis of Cascaded Multipath Fading Channels. Aalto University; Aalto-yliopisto. Consulted at http://urn.fi/URN:ISBN:978-952-60-6563-2.

Zhou, X. & McKay, M. R. (2010). Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation. *IEEE Trans. Veh. Technol.*, 59(8), 3831-3842.

Zhou, X., Song, L. & Zhang, Y. (2016). *Physical layer security in wireless communications*. CRC Press.

Zhu, J., Zou, Y., Wang, G., Yao, Y. D. & Karagiannidis, G. K. (2016). On Secrecy Performance of Antenna-Selection-Aided MIMO Systems Against Eavesdropping. *IEEE Trans. Veh. Technol.*, 65(1), 214-225.

Zou, Y. & Wang, G. (2016). Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack. *IEEE Trans. Ind. Inform.*, 12(2), 780-787.

Zou, Y., Zhu, J., Wang, X. & Leung, V. C. M. (2015). Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network*, 29(1), 42-48.